Doc 9303

Машиносчитываемые проездные документы

Часть 3
Машиносчитываемые официальные проездные документы
Том 2
Спецификации на электронные МСОПД со средствами биометрической идентификации

Утверждено Генеральным секретарем и опубликовано с его санкции

Издание третье — 2008

Международная организация гражданской авиации

Doc 9303

Машиносчитываемые проездные документы

Часть 3
Машиносчитываемые официальные проездные документы
Том 2
Спецификации на электронные МСОПД со средствами биометрической идентификации

Утверждено Генеральным секретарем
и опубликовано с его санкции

Издание третье — 2008

Международная организация гражданской авиации

Опубликовано отдельными изданиями на русском, английском,
арабском, испанском, китайском и французском языках
МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИЕЙ ГРАЖДАНСКОЙ АВИАЦИИ.
999 University Street, Montréal, Quebec, Canada H3C 5H7

Информация о порядке оформления заказов и полный список агентов по продаже и книготорговых фирм размещены на веб-сайте ИКАО www.icao.int.

Издание первое, 1996.
Издание второе, 2002.
Издание третье, 2008.

Doc 9303, Машиносчитываемые проездные документы
Часть 3. Машиносчитываемые официальные проездные документы
Том 2. Спецификации на электронные МСОПД
со средствами биометрической идентификации
Номер заказа: 9303P3-2
ISBN 978-92-9231-310-4

© ИКАО, 2009

Все права защищены. Никакая часть данного издания не может воспроизводиться, храниться в системе поиска или передаваться ни в какой форме и никакими средствами без предварительного письменного разрешения Международной организации гражданской авиации.

ПОПРАВКИ

Об издании поправок сообщается в дополнениях к *Каталогу изданий ИКАО;* Каталог и дополнения к нему имеются на веб-сайте ИКАО www.icao.int. Ниже приводится форма для регистрации поправок.

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ		
№	Дата	Кем внесено

ИСПРАВЛЕНИЯ		
№	Дата	Кем внесено

ОГЛАВЛЕНИЕ

Страница

Страница

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

В части 3 настоящего тома документа Doc 9303 используются следующие сокращения и термины. Этот список дополняет содержащиеся в томе 1 сокращения и термины.

Сокращение	**Полная форма**
ДОК	Директория открытых ключей
МСПД	Машиносчитываемый проездной документ, соответствующий спецификациям частей 1, 2 или 3 документа ИКАО Doc 9303.
Электронный МСПД	МСПД (паспорт, виза или карточка) с заделанной в него бесконтактной ИС, который может использоваться для биометрической идентификации владельца МСПД в соответствии со стандартами, изложенными в соответствующей части документа ИКАО Doc 9303.
Электронный МСОПД	Машиносчитываемый официальный проездной документ с заделанной в него бесконтактной ИС, который может использоваться для биометрической идентификации владельца МСОПД в соответствии со стандартами, изложенными в части 3 документа ИКАО Doc 9303.
AID	Идентификатор приложения
APDU	Протокольный блок данных приложения
CA	Сертифицирующий полномочный орган
CID	Идентификатор карточки
CRL	Список отзыва сертификатов
DES	Стандарт кодирования данных
DO	Объект данных
DSA	Алгоритм цифровой подписи
EAL	Уровень гарантии оценки
EEPROM	Электрически стираемая программируемая постоянная память. Технология энергонезависимой памяти, когда данные могут быть электрически стерты или перезаписаны.
FRR	Коэффициент ложного отказа
IC	Интегральная схема
ICC	Карточка на интегральной схеме
IFD	Устройство интерфейса
JPEG	Стандарт на сжатие изображений, применяемый, в частности, в технологии хранения изображений лица.
JPEG 2000	Обновленная версия стандарта JPEG
LDS	Логическая структура данных
MAC	Код аутентичности сообщения

Сокращение	Полная форма
MRZ	Машиносчитываемая зона
NAD	Адрес узла
NIST	Национальный институт стандартов и технологии
NTWG	Рабочая группа по новым технологиям
OCR	Оптическое распознавание знаков
PCD	Устройство соединения через малый зазор
PICC	Карточка на интегральной схеме с индуктивной связью через малый зазор
PID	Создатель контрольных биометрических данных
PKI	Инфраструктура открытых ключей
RSA	Асимметричный алгоритм, изобретенный Роном Ривестом, Ади Шамиром и Леном Адлеманом. Его применение основано на том факте, что умножить два очень больших простых числа легко, но трудно факторизировать их произведение.
SHA	Алгоритм безопасного хэширования
SM	Безопасный обмен сообщениями
TAG	Техническая консультативная группа
UID	Уникальный идентификатор
WSQ	Коротковолновое скалярное квантование
X.509v3	Цифровой сертификат – ITU-T. Международно признанный электронный документ, используемый для подтверждения идентичности и принадлежности открытого ключа по сети связи. Он содержит имя издателя сертификата, идентификационную информацию о нем и его цифровую подпись.

Термин	Определение
Алгоритм	Определенный математический процесс вычисления; набор правил, следуя которым будет получен заданный результат.
Алгоритм безопасного хэширования (SHA)	Функция хэширования, разработанная NIST и опубликованная в 1993 году в качестве федерального стандарта обработки информации
Алгоритм цифровой подписи (DSA)	Ассиметричный алгоритм, опубликованный NIST в качестве федерального стандарта обработки информации (FIPS) в 1991 году и пересмотренный им в 1993 году. Этот алгоритм обеспечивает только функцию цифровой подписи.
Ассиметричность	Различные ключи, которые должны быть на каждом конце линии связи.
Ассиметричные ключи	Отдельная, но интегрированная пара ключей пользователя, состоящая из одного открытого ключа и одного закрытого ключа. Каждый ключ является односторонним, а это означает, что ключ, использованный для шифрования информации, не может быть использован для дешифрования этой же информации.

Термин	**Определение**
Ассиметричный алгоритм	Тип криптографической операции с использованием одного ключа для шифрования открытого текста и второго ключа для дешифрования соответствующего шифрованного текста. Эти два ключа связаны друг с другом и называются парой ключей.
Атака методом грубой силы	Испытание и перебор всех возможных ключей шифрования до тех пор, пока в результате не будет найден ключ, дающий открытый смысловой текст.
Аутентификация	Процедура подтверждения подлинности предъявленной идентификационной информации в процессе электронной транзакции.
База данных	Хранилище биометрических шаблонов и соответствующей информации о конечном пользователе в электронном формате.
Байт	Последовательность восьми битов, которые, как правило, обрабатываются как единое целое.
Бесконтактная интегральная схема	Электронный микрочип, соединенный с антенной, позволяющий производить передачу данных между чипом и кодирующим/считывающим устройством без необходимости в прямом электрическом контакте.
Биометрическая система	Автоматизированная система, способная: 1. брать биометрический образец у конечного пользователя для МСПД; 2. извлекать биометрические данные из биометрического образца; 3. сравнивать конкретные биометрические данные с данными в одном или нескольких контрольных шаблонах; 4. определять, насколько точно совпадают данные из этих двух источников; 5. указывать, была ли достигнута идентификация или верификация личности.
Биометрический образец	Единственные исходные данные, представляющие собой уникальные биометрические характеристики зарегистрированного пользователя, забранные биометрической системой.
Биометрический шаблон	Извлеченные и сжатые данные из взятого биометрического образца.
Бит	Двоичная цифра. Минимально возможная единица исчисления информации в цифровом коде.
Блок	Строка или группа битов, которыми оперирует блочный алгоритм.
Блочный алгоритм	См. блочный шифр.
Блочный шифр	Алгоритмы, которые преобразовывают открытый текст в блоках (строки или группы) битов.
Бутстрэппинг	Метод проверки достоверности набора данных.
Валидация	Процесс демонстрации того, что рассматриваемая система во всех отношениях соответствует техническим требованиям к этой системе.

Термин	Определение
Верификация/ верифицировать	Процесс сравнения представленного биометрического образца с биометрическим контрольным шаблоном одного зарегистрированного пользователя, в отношении которого предъявляется идентификационная информация, с целью определить, совпадает ли он с шаблоном зарегистрированного пользователя. Ср. с термином "идентификация".
Владелец	Обладающее электронным МСПД лицо, которое предоставляет биометрический образец для верификации или идентификации, предъявляя правильную или ложную идентификационную информацию. Лицо, взаимодействующее с биометрической системой для занесения в нее или проверки его идентификационной информации.
Галерея	База данных, содержащих биометрические шаблоны ранее зарегистрированных лиц, которые могут просматриваться с целью обнаружения пробника.
Глобальная интероперабельность	Способность систем проверки (автоматизированных или неавтоматизированных) различных государств мира принимать данные и производить обмен ими, обрабатывать данные, полученные из систем других государств, и использовать эти данные при проведении проверок в соответствующих государствах.
Дальность считывания	Практически возможное максимальное расстояние действия между бесконтактной ИС с антенной и считывающим устройством.
Директория/ директория открытых ключей (ДОК)	Хранилище информации. Как правило, директория конкретной PKI служит хранилищем сертификатов открытых ключей шифрования, выданных сертифицирующим полномочным органом PKI, вместе с другой информацией о клиентах. В директории также хранятся кросс-сертификаты, списки отзыва сертификатов и списки аннулированных удостоверяющих центров.
Закрытый ключ	Криптографический ключ, известный только пользователю, который используется в криптографии открытого ключа для дешифрования или подписи.
Занесение в систему	Процесс взятия у лица биометрических образцов и последующая подготовка и хранение биометрических контрольных шаблонов, идентифицирующих данное лицо.
Заполнение	Добавление дополнительных битов до требуемой длины с обеих сторон строки данных.
Запоминающее устройство для данных	Средство хранения данных в таком документе, как МСПД. В томе 2 части 1 и 3 документа ИКАО Doc 9303 указано, что в электронном машиносчитываемом документе данные будут храниться на бесконтактной интегральной схеме.
Зарегистрированный пользователь	Лицо, обратившееся за получением электронного МСПД.
Захват	Метод взятия биометрического образца у конечного пользователя.
Защищенное сообщение	Сообщение, которое защищено от незаконного изменения или подмены.

Термин	**Определение**
Идентификатор	Уникальный ряд данных, используемый в биометрической системе в качестве ключа к идентификации лица и его соответствующих атрибутов. Примером идентификатора служит номер МСПД.
Идентификатор приложения (AID)	Элемент данных, используемый для уникальной идентификации приложения в карточке. Он состоит из относительного идентификатора (RID) и собственного добавления к идентификатору (PIX).
Идентификатор соединения ("Nonce")	В технике обеспечения безопасности специальный код – это "число, используемое один раз". Это часто произвольное или псевдо произвольное число, установленное в протоколе аутентификации, с целью гарантировать, чтобы старые сообщения не могли быть повторно использованы для "взлома защиты путём замещения оригинала". Например, специальные идентификаторы соединения используются в обеспечиваемом дайджестом HTTP установлении подлинности доступа для расчета дайджеста MD5 пароля. Индикаторы соединения различные каждый раз, когда присутствует код 401 аутентификации "запрос/ответ", что делает "взлом защиты путём замещения оригинала" практически невозможным (источник: wikipedia.org).
Идентификация/ идентифицировать	Процесс сравнения представленного биометрического образца со всеми биометрическими контрольными шаблонами в файле с целью определить совпадает ли он с одним из шаблонов и если совпадает, то установить личность владельца электронного МСПД, чей шаблон оказался подходящим. Ср. с термином "верификация".
Извлечение	Процесс преобразования взятого биометрического образца в биометрические данные с тем, чтобы их можно было сравнить с контрольным шаблоном.
Изображение	Воспроизведение биометрического параметра, обычно фиксируемого при помощи видеоаппаратуры, фотокамеры или сканирующего устройства.
Инициализация	(Смарт-карты). Процесс заполнения постоянной памяти (EEPROM и т.п.) данными, которые одинаковы для большинства карт, а также минимальным количеством уникальных для каждой конкретной карты элементов (например, серийный номер и ключи персонализации ICC).
Интеграция систем	Процесс, с помощью которого лицевая, внутренняя и контактная системы карточки владельца и приложения интегрируются друг с другом.
Интерфейс	Стандартное техническое определение связи между двумя компонентами.
Инфраструктура открытых ключей (PKI)	Набор стратегий, процессов и технологий, используемых для верификации, занесения в систему и сертификации пользователей системы поддержки безопасности. В PKI для защиты связи используется криптография открытого ключа и практика сертификации ключа.
Карточка на интегральной(ых) схеме(ах) (карточка ИС, ICC)	Карточка, в которую встроены одна или несколько ИС.
Ключ	См. "Криптография открытого ключа".

Термин	Определение
Код аутентичности сообщения (MAC)	MAC представляет собой краткую форму сообщения, которая прилагается к самому сообщению. MAC не может быть вычислен или верифицирован, если не известен секрет. Он прилагается отправителем и верифицируется получателем, который может обнаружить подделку сообщения.
Конечный пользователь	Лицо, взаимодействующее с биометрической системой для занесения в нее или проверки его идентификационной информации.
Контрольный биометрический шаблон	Набор данных, которые определяют биометрические показатели лица, в дальнейшем используемые в качестве основы для сравнения с представляемым(и) биометрическим(и) образцом(ами).
Коротковолновое скалярное квантование	Способ сжатия данных, применяемый, в частности, для хранения изображений отпечатков пальцев.
Коэффициент ложного допуска (FAR)	Вероятность того, что биометрическая система ошибочно идентифицирует лицо или не сможет отказать самозванцу.
Коэффициент ложного несовпадения	Альтернатива "коэффициенту ложного отказа"; используется во избежание путаницы в прикладных программах, отказывающих предъявителю при совпадении его биометрических данных с биометрическими данными зарегистрированного пользователя.
Коэффициент ложного отказа (FRR)	Вероятность того, что биометрическая система не сможет идентифицировать зарегистрированного пользователя или произвести верификацию правильности предъявленной идентификационной информации зарегистрированного пользователя.
Коэффициент ложного совпадения	Альтернатива "коэффициенту ложного допуска"; используется во избежание путаницы в прикладных программах, отказывающих предъявителю при совпадении его биометрических данных с биометрическими данными зарегистрированного пользователя.
Криптография	Наука о преобразовании информации в зашифрованную и неразборчивую с помощью алгоритма и ключа.
Криптография открытого ключа	Вид асимметричного шифрования, когда все стороны владеют парами ключей, один из которых закрытый, а второй открытый, для использования при шифровании и цифровой подписи данных.
Личность	Совокупность отличительных персональных и физических признаков, данных и качеств, позволяющих однозначно идентифицировать лицо среди других лиц. В биометрической системе личность обычно устанавливается при регистрации лица в системе с использованием так называемых "исходных документов", таких как свидетельство о рождении и свидетельство о гражданстве.
Логическая структура данных (LDS)	Описание того, как должны записываться и форматироваться данные на бесконтактной ИС электронного МСПД.
Ложный допуск	Случай, когда биометрическая система ошибочно идентифицирует лицо или ошибочно верифицирует личность самозванца по предъявленной идентификационной информации.

Термин	**Определение**
Маркерное изображение	Фотография владельца МСПД, обычно представляющая собой изображение анфас, размеры которого скорректированы для выдерживания фиксированного расстояния между глазами. Оно может быть также слегка повернуто так, чтобы воображаемая горизонтальная линия между центрами глаз была параллельна верхней кромке прямоугольной фотографии, если этого не было достигнуто, когда делалась или вводилась оригинальная фотография. (См. п. 12 раздела II настоящего тома).
Мастер-ключ	Источник генерации цепи ключей.
Машиносчитываемый проездной документ (МСПД)	Проездной документ, соответствующий спецификациям частей 1, 2 или 3 документа ИКАО Doc 9303.
Модуль ИС	Заделанный в ICC блок, состоящий из интегральной схемы (ИС), ее держателя и контактов. Серийный номер интегральных схем: общий номер для всей партии ИС, увязанный с определенным местом в шаблоне (используется в процессе изготовления).
Невозможность занесения в систему	Неспособность биометрической системы зарегистрировать потенциального конечного пользователя.
Невозможность получения информации	Неспособность биометрической системы получить необходимый биометрический параметр для регистрации лица.
Негласный съем информации	Несанкционированный перехват передаваемых данных.
Обмен ключами	Процесс передачи сеансовых ключей в руки осведомленных лиц.
"Один к нескольким"	Сочетание идентификации "один ко многим" и верификации "один к одному". Как правило, процесс "один к нескольким" предполагает сравнение представленного биометрического образца с небольшим количеством биометрических контрольных шаблонов в файле. На него обычно делается ссылка при сопоставлении со списком "особого внимания", где указываются лица, требующие тщательной проверки идентификационной информации, или известные преступники, террористы и т. д.
"Один к одному"	Синоним термина "верификация".
"Один ко многим"	Синоним термина "идентификация".
Оперативная память (RAM)	Энергозависимая память с произвольным доступом, используемая в интегральных схемах, которым необходимо энергопитание для сохранения данных.
Операционная система	Программа управления различными прикладными программами, используемыми компьютером.
Ответ	Сообщение, возвращенное подчиненным компонентом главному после обработки команды, полученной подчиненным компонентом.
Открытый ключ	Открытый компонент интегрированной асимметричной пары ключей, используемый для шифрования или верификации информации.

Термин	Определение
Оценка	Число по шкале оценки от низкой до высокой, определяющее степень совпадения данных биометрического пробника (отыскиваемого лица) с конкретными данными из галереи (ранее зарегистрированного лица).
Пара ключей	Пара цифровых ключей, а именно, один открытый и один закрытый, которые используются для шифрования и подписи цифровой информации.
Персональные идентификационные данные	Информация, связанная с владельцем карточки и используемая системой идентификации личности.
Персональный идентификационный номер (PIN)	Цифровой код защиты, используемый как механизм местной верификации "один к одному", с целью убедиться, что владелец карточки действительно является тем лицом, которому разрешен доступ или выполнение конкретных функций, например, право открытия определенной информации на карточке.
Подписывающий документы орган	Орган, который выдает биометрический документ и удостоверяет, что внесенные в этот документ данные являются подлинными, и делает это таким образом, чтобы можно было обнаружить мошеннические изменения.
Политика обеспечения безопасности системы	Свод законов, правил и практики, регулирующих то, как осуществляется управление уязвимой информацией и другими ресурсами, а также их защита и распространение в рамках конкретной системы.
Полное изображение лица (анфас)	Фотография владельца МСПД, изготовленная в соответствии со спецификациями, изложенными в разделе IV тома 1 части 3 документа ИКАО Doc 9303.
Полномочный орган регистрации	Лицо или организация, несущие ответственность за идентификацию и аутентификацию заявителя на получение цифрового сертификата. Полномочный орган регистрации не выдает и не подписывает сертификаты.
Порог	Контрольная оценка, выше которой степень соответствия между хранящимся биометрическим параметром и лицом считается допустимой, а ниже – неприемлемой.
Постоянная память только для чтения (ROM)	Энергонезависимая память, которая заполняется один раз, как правило, в ходе изготовления ИС. Она применяется для хранения операционных систем и алгоритмов, используемых полупроводником карточки на интегральной схеме во время транзакции.
Проверка	Действия государства, связанные с проверкой электронного МСПД, предъявленного лицом (владельцем электронного МСПД), совершающим поездку, и верификацией аутентичности.
Проверка на совпадение[1]	Процесс сравнения биометрического образца с ранее внесенным в память шаблоном (т.е. контрольным биометрическим шаблоном) и оценивания уровня сходства. Решение о принятии или отклонении принимается, исходя из того, превышает ли определенный уровень сходства установленное предельное значение.

1 Это определение применимо только в контексте биометрической системы.

Термин	**Определение**
Проверочная система	Система, используемая для проверки электронных МСПД какими-либо государственными или частными органами, например, органами пограничного контроля, авиакомпаниями, другими эксплуатантами транспорта и финансовыми учреждениями, которые должны проверять действительность электронного МСПД и использовать такой документ для верификации личности.
Проверять на совпадение/проверка на совпадение	Процесс сравнения биометрического образца с ранее записанным шаблоном и оценивания уровня сходства.
Произвольный доступ	Способ хранения данных, при котором конкретные элементы данных можно извлекать без необходимости последовательно просматривать все хранящиеся данные.
Протокольный блок данных приложения (APDU)	Стандартный протокол обмена сообщениями между считывателем карточек и смарт-картой.
Прямой захват	Процесс взятия биометрического образца путем взаимодействия между владельцем электронного МСПД и биометрической системой.
Размер шаблона	Объем памяти компьютера, занимаемый биометрическими данными.
Расшифровка	Метод восстановления зашифрованного файла в его первоначальное состояние с помощью ключа.
Регистрация	Процесс внесения идентификационной информации лица в биометрическую систему, увязки уникального идентификатора с данной личностью, а также сбора и записи соответствующих атрибутов лица в системе.
Регистрация (лица)	Получение достаточных доказательств личности предполагаемого владельца карточки с помощью обычных средств, включая возможное получение характерных атрибутов (например, если это необходимо для особого электронного сервиса). Регистрация заключается в определенном уровне идентификации личности.
Самозванец	Лицо, предъявляющее биометрический образец в преднамеренной или невольной попытке выдать себя за другое лицо.
Сертификат	Цифровой документ, подтверждающий аутентичность открытого ключа.
Сертификат открытого ключа	Информация об открытом ключе юридического лица, подписанная сертифицирующим полномочным органом и поэтому постоянно упоминаемая.
Сертифицирующий полномочный орган (CA)	Надежный орган, выдающий цифровые сертификаты для PKI.
Симметричный алгоритм	Тип шифрования с использованием одного и того же ключа или набора ключей как для шифрования открытого текста, так и для расшифровки соответствующего зашифрованного текста.
Система	Специальная установка информационных технологий (ИТ) с определенными целями и оперативной средой.

Термин	Определение
Система открытого ключа	Криптографический метод с использованием пары ключей, один из которых закрытый, а второй – открытый. Если шифрование произведено с использованием открытого ключа, то для дешифрования необходимо применять соответствующий закрытый ключ, и наоборот.
Система персональной идентификации	Методы, используемые для подтверждения идентификации личности владельца карты.
Сообщение	Минимальный набор информации, имеющей смысл, которая передается от отправителя к получателю. Эта информация может состоять из одной или нескольких транзакций карточки или информации, связанной с карточкой.
Сопоставление биометрических данных	Процесс с использованием алгоритма, в ходе которого сравниваются шаблоны, полученные на основе биометрических контрольных данных, с непосредственно снимаемыми биометрическими данными, в результате чего определяется их соответствие или несоответствие.
Составная биометрическая характеристика	Использование более одного биометрического параметра.
Список отзыва сертификатов (CRL)	Список отзыва сертификатов в рамках данной инфраструктуры.
Стандарт кодирования данных (DES)	Метод кодирования данных с использованием специального алгоритма.
Схема формирования электронно-цифровой подписи (DSS)	Стандарт цифровой подписи, включая DSA, утвержденный NIST, который определен в NIST FIPS PUB 186, май 1994 года, Министерство торговли США.
Управление ключами	Процесс, с помощью которого криптографические ключи предоставляются для использования между взаимодействующими уполномоченными сторонами.
Уровень гарантии оценки (EAL)	Гарантия соответствия требованиям, определенным в "Common Criteria" международного стандарта, действующего с 1999 года. Повышение уровней гарантии оценки определяет повышение требований к гарантии в компьютерных системах.
Устройство интерфейса	Любой терминал, устройство связи или установка, с которыми карточка ИС электрически связана во время операции.
Учет количества повторных операций ввода идентификационных данных	Число последовательных отвергнутых вводов персональных идентификационных данных владельцем карточки.

Термин	**Определение**
Хэш	Математическая формула, с помощью которой сообщение произвольной длины переводится в уникальную строку чисел фиксированной длины (обычно 160 бит), известную под названием "краткая форма сообщения", которая в этом виде представляет первоначальное сообщение. Хэш является односторонней функцией, а это означает, что невозможно произвести обратный процесс и вернуть первоначальное сообщение. Кроме того, хэш-функция не обеспечивает получения одинаковой сжатой формы сообщения из двух различных источников.
Шаблон/контрольный шаблон	Данные, представляющие собой биометрические показатели зарегистрированного пользователя, используемые биометрической системой для сравнения с представляемыми впоследствии биометрическими образцами.
Шифрование	Тайнопись на основе использования ключа или в соответствии с набором заранее определенных правил или символов.
Энергонезависимое устройство памяти	Полупроводниковая память, которая сохраняет информацию при отключении питания (т.е. ROM, EEPROM).
SHA	См. "Алгоритм безопасного хэширования".
SHA-1	Пересмотренная в 1994 году версия SHA, которая считается более безопасной.

РАЗДЕЛ I

ВВЕДЕНИЕ

1. ВВЕДЕНИЕ К ТОМУ 2

1.1 Третье издание части 3 документа Doc 9303 состоит из двух томов. В томе 1 определяются спецификации на базовый машиносчитываемый официальный проездной документ (МСОПД), в котором машиносчитываемые данные представлены в формате оптического распознавания знаков (OCR). Все государства, выдающие машиносчитываемые официальные проездные документы (МСОПД), изготавливают их в соответствии со спецификациями, изложенными в томе 1.

1.2 Количество данных, которое может храниться в формате OCR в машиносчитываемом проездном документе (МСПД), ограничено. Государства нуждаются в том, чтобы хранить в документе как можно больше данных о владельце документа и данных, подтверждающих действительность документа. Основная причина, почему необходимо хранить в нем большое количество данных, заключается в том, что требуется обеспечивать биометрическую идентификацию владельцев таких документов и таким образом усилить борьбу с нелегальной иммиграцией и терроризмом. Государства принимают меры по облегчению прохождения формальностей в иммиграционных пунктах, если проездные документы пассажира содержат биометрические идентификационные данные, соответствующие спецификациям ИКАО.

1.3 В томе 1 третьего издания части 3 документа Doc 9303 обновлены спецификации на машиносчитываемые официальные проездные документы, ранее опубликованные во втором издании (2002 г.). Эти изменения и добавления были внесены главным образом в результате принятия решения об обеспечении глобальной интероперабельности таких документов путем их стандартизации на основе применения в конкретном сочетании единой технологии хранения большого объема данных и системы биометрической идентификации. Это привело к внесению некоторых изменений в том 1, в частности более жестких спецификаций в отношении фотографии владельца, для того, чтобы даже если государство первоначально не использует новые технологии, тем не менее, создается база данных, которая пригодится после того, как государство обновит свою систему. Кроме того, во втором издании приводилось описание ряда биометрических систем и технологий хранения данных, которые не соответствуют новому глобальному интероперабельному стандарту. Государство, конечно, свободно в своем выборе продолжать использовать эти технологии в своих или согласованных на двусторонней основе целях, хотя они не будут глобально интероперабельными. Содержащиеся в настоящем томе 2 спецификации на новую интероперабельную систему предназначены для использования только теми государствами, которые хотят выдавать электронные МСОПД со средствами биометрической идентификации. Такие государства должны соблюдать спецификации, изложенные в *обоих* томах в целях обеспечения соответствия стандартам, изложенным в части 3 документа Doc 9303.

1.4 Содержащиеся в настоящем документе спецификации были разработаны в результате многолетних детальных исследований, которые Рабочая группа по новым технологиям (NTWG) Технической консультативной группы ИКАО по машиносчитываемым проездным документам (TAG/MRTD) начала проводить в 1998 году. В ходе исследований изучались различные системы биометрической идентификации, и при этом основное внимание уделялось упрощению формальностей для лица, совершающего поездку, при подаче заявки и получении МСПД со средствами биометрической идентификации и использовании такого документа для поездок в другие

государства. Применяемые в государствах законы о неприкосновенности личной жизни граждан и требование о том, чтобы биометрические средства были приемлемы для владельца МСПД, в значительной мере повлияли на выбор лица владельца в качестве глобального интероперабельного биометрического параметра, так как лицо в форме фотографии является повсеместно принятым средством идентификации в проездных документах. Опознание по лицу требует отражения соотношения ряда размеров между чертами лица, например расстояния между глазами. Кроме того, проводится сравнительная проверка данных лица, получившего МСПД, которые были зарегистрированы в момент выдачи, и данных лица[1], представившего самого себя для поездки или въезда в государство. Эти взаимоотношения могут быть математически сокращены до "шаблона", требующего относительно небольшой емкости памяти. К сожалению "шаблоны", используемые различными конкурирующими изготовителями систем опознания черт лица, несовместимы. С той целью, чтобы государства могли свободно выбрать наиболее предпочтительную для них систему опознавания по чертам лица, NTWG решила, что в документе лица, которому был выдан МСПД, должна быть фотография относительно высокой резолюции. Хотя опознавание по чертам лица служит основным глобально интероперабельным биометрическим средством, тем не менее, NTWG подтвердила, что некоторые государства желают использовать несколько биометрических параметров. Многие государства располагают обширными базами данных с отпечатками пальцев, которые они могут пожелать использовать с целью верификации личности путешествующего. В качестве второй альтернативы все большее признание получает опознание по радужной оболочке глаза как надежного метода идентификации. Хотя с технической точки зрения это заслуживает одобрения, тем не менее, применение метода опознания по отпечатку пальца или радужной оболочке глаза связано с довольно обширным и занимающим много времени сбором биометрических данных как на этапе первоначального ввода в систему при выдаче МСПД, так и в порту въезда. Поэтому NTWG приняла решение рекомендовать использование методов опознания по отпечатку пальца и радужной оболочке глаза в качестве факультативных вторичных средств биометрической идентификации. Кроме того, исходя из предлагаемого хранения изображений, государство сможет выбирать поставщика системы опознания по отпечатку или радужной оболочке глаза, так как шаблоны разных изготовителей несовместимы.

1.5 Степень свободы выбора системы опознавания черт лица и дополнительных систем опознавания по отпечатку пальца и радужной оболочке глаза определяется требуемой емкостью памяти для хранения данных. В прошлом несколько предлагаемых технологий хранения данных были отклонены вследствие того, что для этого требовалась очень большая емкость памяти для хранения данных. Хотя предлагалось несколько вариантов, тем не менее, NTWG приняла решение, что для создания глобально интероперабельной системы в документе Doc 9303 должна быть определена единая технология хранения данных. После тщательного изучения этого вопроса NTWG приняла решение выбрать для этого бесконтактную интегральную схему (ИС), соответствующую стандарту ИСО/МЭК 14443. Эта технология заключается в обеспечении связи между модулем ИС (ИС с прикрепленной антенной), заделанным в МСПД, и считывателем, расположенным на расстоянии 10 см (3,9 дюйма). Эта технология отличается следующими преимуществами:

— Технология хорошо зарекомендовала себя в других областях.

— Существует значительное число изготовителей подходящих ИС с различным объемом данных и компаний по комплектации, способных конструировать модуль ИС.

1. Во всех случаях, когда в настоящем документе употребляются грамматические формы мужского рода, их следует понимать как относящиеся к лицам как мужского, так и женского пола.

— Применение технологии ИСО/МЭК 14443 не требует точного размещения МСПД на считывателе, а близкое расстояние для считывания означает, что существует лишь небольшой риск несанкционированного считывания данных, хранящихся на ИС, но при условии, что в считывателе используется адекватное электромагнитное экранирование и соответствующие средства связи.

1.6 Емкость памяти для хранения данных на ИС установлена в объеме как минимум 32 кб (килобайта), что вполне достаточно для хранения обязательного изображения лица и, что также обязательно, дублирующих данных МСЗ. Однако факультативное хранение более чем одного изображения лица и/или изображений отпечатка пальцев/радужной оболочки глаз требует значительно большей емкости памяти для хранения данных.

1.7 В стандарте ИСО/МЭК 14443 определены два альтернативных типа бесконтактной ИС, а именно: A и B. Содержащиеся в настоящем томе спецификации позволяют использовать любой из этих типов, что делает необходимым наличие в пунктах въезда считывателей, способных взаимодействовать с ИС любого из этих типов.

1.8 Важно обеспечивать хранение данных в стандартном формате, чтобы эта система была глобально интероперабельной. Поэтому NTWG разработала логическую структуру данных (LDS), которая определяет то, каким образом широкий диапазон данных может храниться в стандартизированных группах. В ходе разработки LDS Рабочая группа по новым технологиям (NTWG) стремилась добиться, чтобы любое государство могло обеспечить хранение не только биометрических данных, но также любых других данных, которые оно считает связанными с владельцем или подтверждением действительности МСПД, исходя при этом только из емкости памяти для хранения данных, обеспечиваемой выбранной ИС. Поэтому было принято положение, предусматривающее хранение одного или нескольких шаблонов для распознавания черт лица в дополнение к нескольким изображениям лица, а также изображениям и шаблонам отпечатка пальца и/или радужной оболочки глаза владельца. Разрешается хранить такие данные, как имя владельца на языке, в котором не используются латинские знаки, а также использовать диакритические знаки. Единственными обязательными данными, которые должны храниться на ИС, являются данные, дублирующие данные МСЗ, в группе данных 1, *а также* одно изображение лица в группе данных 2 вместе с цифровой подписью с целью гарантировать, что это действительно те данные, которые были вписаны государством выдачи в момент выдачи документа.

1.9 В будущем предполагается принять положение, позволяющее государствам, в число которых не входит государство выдачи, записывать на ИС такие данные, как информация об электронной визе. Однако сейчас это еще не разрешается делать.

1.10 Защита данных на ИС имеет первостепенное значение. Принимающее государство должно быть уверено, что считываемые им с ИС данные не были каким-либо образом изменены после того, как были закодированы государством, выдавшим МСПД. Кроме того, некоторые из таких данных нуждаются в защите от несанкционированного доступа по той причине, что данные могут быть использованы в мошеннических целях или потому что законы многих государств о неприкосновенности личной жизни запрещают несанкционированный доступ к некоторым видам персональных данных. В связи с этим Специальная рабочая группа, созданная NTWG, разработала соответствующие уровни обеспечения защиты и неприкосновенности личной жизни, которые должны соблюдаться путем использования цифровых подписей.

1.11 В 2003 году TAG/MRTD официально представила ИКАО рекомендацию, состоящую из четырех частей. Изображение лица в виде фотографии высокой четкости, хранящееся на бесконтактной ИС, отвечающей стандарту ИСО/МЭК 14443, типы A или B, должно быть глобальным биометрическим стандартом. Нашло также поддержку предложение об использовании отпечатка пальца и радужной оболочки глаза, хранящихся в виде изображений, в качестве вторичных биометрических параметров. Биометрические параметры, а также дубликаты данных МСЗ и целый ряд других данных, должны храниться на ИС в соответствии с логической структурой данных и

требованиями к обеспечению защиты и неприкосновенности личной жизни. Эта рекомендация была принята в качестве рабочего плана ИКАО.

1.12 В настоящем томе этому решению придается официальный статус в виде детальных спецификаций, изложенных в последующих разделах. В разделе II *"Применение средств биометрической идентификации"* определяется метод захвата и использования биометрических данных и излагаются требования к бесконтактной ИС, используемой для хранения данных. В разделе III *"Логическая структура данных"* определяется метод хранения данных на ИС, а в разделе IV *"Инфраструктура открытых/закрытых ключей"* определяются система и процедуры, используемые для защиты данных на ИС, и обеспечение соответствующего ограничения доступа к данным.

1.13 ИКАО признательна за помощь, которая была оказана ИСО в процессе разработки этого узкоспециализированного стандарта. Том 2 представлен ИСО для получения утверждения ею в качестве международного стандарта.

1.14 Сложилось мнение, что реализация содержащихся в настоящем документе спецификаций требует участия высококвалифицированных технических специалистов из числа тех сотрудников государств и их подрядчиков, которые могут быть привлечены к работе по созданию электронных МСОПД и систем захвата, кодирования и считывания хранимых данных и их использования в процессе биометрической верификации и идентификации. Поэтому TAG/MRTD создала сеть различных специалистов, работающих в органах государств, которые уже внедрили такие системы. К таким специалистам можно обращаться за консультациями через секцию ИКАО по авиационной безопасности и упрощению формальностей на sfp@icao.int.

2. ОПРЕДЕЛЕНИЯ И ТЕРМИНЫ

Глоссарий терминов и их определений приводится в начале этого тома. С дополнительными терминами и определениями, имеющими отношение ко всем МСПД, можно ознакомиться в томе 1.

3. ДОПОЛНЕНИЕ

К настоящему стандарту в форме документа Doc 9303 ИКАО будет периодически выпускать "Дополнение к документу Doc 9303". В Дополнение будет включаться информация, предназначенная для разъяснения, развития или конкретизации вопросов, касающихся стандартов на проездные документы, а также для исправления ошибок, выявленных в ходе их внедрения. Предполагается, что содержащаяся в Дополнении информация будет расширять соответствующий инструктивный материал документа Doc 9303, а также технических докладов, выпущенных ИКАО. Дополнение будет выпускаться на постоянной и единообразной основе.

Спецификации документа Doc 9303 всегда следует рассматривать в сочетании с дополнительной информацией, содержащейся в последнем выпущенном дополнении, которое будет размещаться на веб-сайте ИКАО http://www.icao.int/mrtd.

Примечание. Сложилось мнение, что могут возникнуть ситуации, когда электронный МСОПД не будет правильно взаимодействовать со считывателем на пограничном пункте. Это может произойти по нескольким причинам, только одна из которых может быть сбой электронного МСОПД. ИКАО обращает внимание на то, что даже если электронный МСОПД не поддается считыванию, тем не менее, он остается действительным документом. Однако сбой в

считывании может произойти в результате мошеннического акта, и принимающему государству следует установить процедуры действий в таких случаях, которые должны включать более жесткие меры проверки документа и его владельца, а также допускать, что может произойти сбой без каких-либо мошеннических намерений.

4. КЛЮЧЕВЫЕ СЛОВА

В настоящем томе 2 используются следующие ключевые слова для обозначения требований.

Слова "ДОЛЖЕН", "НЕ ДОЛЖЕН", "ТРЕБУЕТСЯ", "SHALL" – в русском языке передается глаголом в настоящем времени, "SHALL NOT" – в русском языке передается о*трицательной формой глагола* в *настоящем времени*, "СЛЕДУЕТ", "НЕ СЛЕДУЕТ", "РЕКОМЕНДУЕТСЯ", "МОЖЕТ" и "ФАКУЛЬТАТИВНО" пишутся заглавными буквами, и их следует понимать так, как указано в RFC 2119:

ДОЛЖЕН Это слово или термины "ТРЕБУЕТСЯ" или "SHALL" означают, что данное определение в спецификации является абсолютным требованием спецификации.

НЕ ДОЛЖЕН Эти слова или слова "SHALL NOT" означают, что данное определение в спецификации является абсолютным запрещением.

СЛЕДУЕТ Это слово или прилагательное "РЕКОМЕНДУЕМЫЙ" означают, что могут существовать обоснованные причины в особых обстоятельствах игнорировать отдельный пункт, однако при этом полностью должны осознаваться и тщательно взвешиваться все последствия, прежде чем будет выбран другой курс действий.

НЕ СЛЕДУЕТ Эти слова или слова "НЕ РЕКОМЕНДУЕМЫЙ" означают, что могут существовать обоснованные причины в особых обстоятельствах для особого поведения, допустимого или даже полезного, однако при этом полностью должны осознаваться и тщательно взвешиваться все последствия этого, прежде чем предпринимать какие-либо особые действия, упомянутые в этом объяснении.

МОЖЕТ Это слово или причастие "ФАКУЛЬТАТИВНО" означают, что данный пункт действительно факультативный. Какой-то пользователь может выбрать вариант включения этого пункта потому, что этого требует особое применение или если он считает, что это расширит применение, а другой пользователь может отказаться от этого. Один вид применения, который не включает какого-либо конкретного варианта, ДОЛЖЕН быть готовым взаимодействовать с другим применением, которое включает такой вариант, хотя, возможно, с пониженной функциональностью. Аналогичным образом, применение, которое не включает какой-либо особый вариант, ДОЛЖНО быть готово взаимодействовать с другим видом применения, которое не включает этот вариант (конечно, за исключением характеристик, обеспечиваемых этим вариантом).

Используемые инструктивные указания. Определенные здесь слова повелительного наклонения должны использоваться осторожно и умеренно. В частности, они ДОЛЖНЫ использоваться только тогда, когда это действительно необходимо для обеспечения взаимодействия или сдерживания поведения, которое потенциально может привести к нанесению ущерба (например, ограничение повторных передач). Например, они не должны использоваться для попыток заставить

лиц, занимающихся внедрением, использовать какой-либо конкретный метод, если этот метод не нужен для обеспечения интероперабельности.

Соображения, касающиеся защиты. Эти термины часто используются для определения поведения, имеющего последствия для защиты. Последствия для защиты невыполнения того, что ДОЛЖНО делаться или СЛЕДУЕТ делать, или того, что сделано то, о чем в спецификации говорится, что делаться НЕ ДОЛЖНО, или делать НЕ СЛЕДУЕТ, могут иметь замедленное действие. Авторам документа следует не спеша и внимательно изучить последствия невыполнения рекомендаций или требований для защиты, так как большинство лиц, занимающихся внедрением, не имеют еще достаточного опыта и не принимали участия в рассмотрении вопросов, в результате чего была подготовлена эта спецификация.

В том случае, когда элементы внедряются ФАКУЛЬТАТИВНО, они ДОЛЖНЫ внедряться как это предусмотрено в настоящем томе.

5. СПРАВОЧНЫЕ МАТЕРИАЛЫ

Некоторые положения в перечисленных ниже международных стандартах стали положениями настоящего тома. В случае расхождений между новыми спецификациями, содержащимися в настоящем томе, и перечисленными ниже стандартами в интересах учета конкретных требований к построению машиносчитываемых проездных документов приводимые здесь спецификации ИМЕЮТ преимущественную силу.

FIPS 180-2. Публикация федеральных стандартов по обработке информации (FIPS PUB) 180-2, стандарт хэш-функций защиты (SHS), август 2002 года

FIPS 186-2. Публикация федеральных стандартов по обработке информации (FIPS PUB) 186-2 (+ уведомления об изменении), стандарт на цифровую подпись (DSS), 27 января 2000 года. (Заменяет FIPS PUB 186-1 от 15 декабря 1998 года.)

Doc 9303. Машиносчитываемые проездные документы, часть 1, Машиносчитываемые паспорта (6-е издание, 2006 год).

ИСО 3166-1: 2006. Коды для представления названий стран и единиц их административно-территориального деления. Часть 1. Коды стран

ИСО 3166-2: 2007. Коды для представления названий стран и единиц их административно-территориального деления. Часть *2.* Коды единиц административно-территориального деления

ИСО/МЭК 7816-4: 2005. Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 4. Межотраслевые команды для обмена

ИСО/МЭК 7816-5: 2004. Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 5. Регистрация провайдеров прикладных программ

ИСО/МЭК 7816-6: 2004. Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 6. Элементы межотраслевых данных для обмена информацией (включая доклады о дефектах)

ИСО/МЭК 7816-11: 2004. Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 11. Персональный контроль с помощью биометрических данных

ИСО/МЭК 8825-1: 2003. Информационные технологии. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования

ИСО/МЭК 9796-2: 2002. Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации

ИСО/МЭК 9797-1: 1999. Информационные технологии. Методы обеспечения безопасности. Коды аутентификации сообщений. Часть 1. Механизмы с использованием блочного шифра

ИСО/МЭК 10373-6: 2001. Карточки идентификационные. Методы испытаний. Часть 6. Бесконтактные карточки, обеспечивающие считывание кода при поднесении к считывателю на близкое расстояние (проксимити карточки)

ИСО/МЭК 10373-6: 2001/Amd 1: 2007. Методы испытаний бесконтактных карточек, обеспечивающих считывание кода при поднесении к считывателю на близкое расстояние. (Изменение 1. Методы испытания протокола для проксимити карточек)

ИСО/МЭК 10373-6: 2001/Amd 2: 2003. Методы испытаний бесконтактных карточек, обеспечивающих считывание кода при поднесении к считывателю на близкое расстояние. (Изменение 2. Усовершенствованные методы высокочастотных испытаний RF)

ИСО/МЭК 10373-6: 2001/Amd 4: 2006. Методы испытаний бесконтактных карточек, обеспечивающих считывание кода при поднесении к считывателю на близкое расстояние. (Изменение 4. Методы дополнительных испытаний интерфейса PCD RF и воздействия переменного поля PICC)

ИСО/МЭК 10373-6:2001/Amd 5. Методы испытаний бесконтактных карточек, обеспечивающих считывание кода при поднесении к считывателю на близкое расстояние. (Изменение 5. Скорости передачи в битах fc/64/, fc/32 и fc/16)

ИСО/МЭК 10646: 2003. Информационные технологии. Универсальный многооктетный набор кодированных символов (UCS)

ИСО/МЭК 10918. Информационные технологии. Цифровое уплотнение и кодирование неподвижных изображений с непрерывным спектром тонов

ИСО 11568-2: 2005. Банковское дело. Менеджмент ключей (розничная торговля). Часть 2. Симметричные алгоритмы шифрования, управление их ключами и жизненный цикл

ИСО/МЭК 11770-2: 1996. Информационные технологии. Методы защиты. Управление ключами защиты. Часть 2. Механизмы, использующие симметричные методы

ИСО/МЭК 14443-1: 2000. Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 1. Физические характеристики

ИСО/МЭК 14443-2: 2001. Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 2. Мощность высокочастотного сигнала и сигнальный интерфейс

ИСО/МЭК 14443-2: 2001/AM1: 2005. Карточки идентификационные. Мощность высокочастотного сигнала и сигнальный интерфейс. (Изменение 1. Скорость передачи в битах fc/64, fc/32 и fc/16)

ИСО/МЭК 14443-3:2001. Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 3. Инициализация и предупреждение конфликта на уровне данных

ИСО/МЭК 14443-3: 2001/AM1: 2005. Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 3. Инициализация и антиконфликтность

ИСО/МЭК 14443-4: 2001. Карточки идентификационные. Бесконтактные карточки на интегральных схемах. Карточки с индуктивной связью через малый зазор. Часть 4. Протокол передачи

ИСО/МЭК 15444. Информационные технологии. Система кодирования изображения JPEG 2000

ИСО/МЭК 15946: 2002. Информационные технологии. Методы защиты. Криптографические методы на основе эллиптических кривых

ИСО/МЗК 19794-4: 2005. Информационные технологии. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца

ИСО/МЭК 19794-5: 2005. Информационные технологии. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

ИСО/МЭК 19794-6:2005. Информационные технологии. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза

RFC 2119, С. Бреднер, "Ключевые слова для обозначения уровня требований в RFC", BCP 14 марта 1997 г.

RFC 3279, W. Polk, R. Housley, L. Bassham, “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, April 2002

RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, April 2002

RFC 3369, R. Housley, Cryptographic Message Syntax (CMS), August 2002

RFC 3447, J. Jonsson, B. Kaliski, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”, February 2003

Unicode 4.0.0. Консорциум Уникод. Стандарт "Unicode", версия 4.0.0, установленная *стандартом* Unicode*, версия 4.0* (Boston, MA, Addison-Wesley, 2003. ISBN 0-321-18578-1) (Соответствует стандарту ИСО/МЭК 10646-1, но содержит дополнительные характеристики)

ANSI X9.62:2005, “Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 7 January 1999

РАЗДЕЛ II

ПРИМЕНЕНИЕ СРЕДСТВ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ И ЭЛЕКТРОННОГО ХРАНЕНИЯ ДАННЫХ В МАШИНОСЧИТЫВАЕМЫХ ОФИЦИАЛЬНЫХ ПРОЕЗДНЫХ ДОКУМЕНТАХ

1. СФЕРА ПРИМЕНЕНИЯ

1.1 В разделе II определяются технические спецификации, дополняющие изложенные в томе 1 части 3 документа Doc 9303 базовые спецификации на ПД-1 и ПД-2 для использования государствами, решившими выдавать машиносчитываемые официальные проездные документы с электронной активацией (электронные МСОПД), которые могут использоваться любым принимающим государством, имеющим соответствующее оборудование, для считывания с документа гораздо большего объема данных, касающихся самого МСОПД и его владельца. Они включают обязательные глобально интероперабельные биометрические данные, которые могут вводиться в системы распознавания черт лица и, факультативно, в системы распознавания отпечатков пальцев или радужной оболочки глаза. Эти спецификации ТРЕБУЮТ обеспечивать хранение глобально интероперабельных биометрических данных в форме изображений высокой четкости на бесконтактной интегральной схеме (ИС) большой емкости, содержащей также дубликат закодированных данных МСЗ. Кроме того, спецификации допускают хранение ряда факультативных данных по усмотрению государства выдачи. Поскольку использование бесконтактной интегральной схемы не зависит от размера документа, то все спецификации применимы к электронному формату как ПД-1, так и ПД-2. Различия между форматом ПД-1 и ПД-2 электронного МСОПД связаны с МСЗ в части, касающейся хранения МСЗ на бесконтактной ИС. Эти различия указаны в спецификациях, содержащихся в настоящем томе.

2. ЭЛЕКТРОННЫЙ МСОПД

Примечание. Термины МСПД и электронный МСПД используются в настоящем документе в качестве общего названия всех типов машиносчитываемых проездных документов соответственно в формате оптического распознавания знаков и электронном формате. Термины МСОПД и электронный МСОПД используются только в отношении соответствующих официальных проездных документов. Термины ПД-1 и ПД-2 обозначают два размера МСОПД. Все МСОПД, о которых речь идет в настоящем томе, являются электронными документами.

2.1 *Соответствие спецификациям тома 1 части 3 документа Doc 9303.* МСОПД с электронной активацией (электронный МСОПД) во всех отношениях СООТВЕТСТВУЕТ спецификациям, содержащимся в томе 1 части 3 документа Doc 9303, а также спецификациям, изложенным в настоящем томе.

2.2 *Срок действия электронного МСОПД.* Срок действия электронного МСОПД устанавливается по усмотрению государства выдачи; однако, принимая во внимание ограниченную износостойкость документов и изменение со временем внешнего вида владельца документа, РЕКОМЕНДУЕТСЯ, чтобы срок действия документа составлял не более десяти лет. Государства могут рассмотреть вопрос об установлении более короткого срока с целью реализации возможности постепенной модернизации электронного МСОПД по мере развития технологии.

3. ЧИП В СИМВОЛЕ

3.1 *Визуальная индексация того, что МСПД является электронным МСОПД.* Все электронные МСОПД ИМЕЮТ следующий символ (рис. II-1):

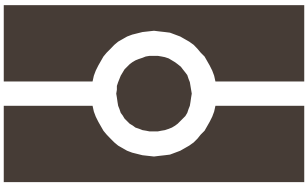


Рис. II-1

Электронный файл символа имеется на веб-сайте ИКАО. Символ может фигурировать только на МСОПД, содержащем бесконтактную интегральную схему с емкостью памяти не менее 32 кб, на которой хранятся, как минимум, закодированные в соответствии с логической структурой данных (раздел III настоящего тома) данные МСЗ, входящие в группу данных 1, и изображение лица в соответствии со спецификациями этого раздела в группе данных 2, причем все внесенные данные защищаются цифровой подписью, как указано в разделе IV настоящего тома. Если МСОПД не отвечает этим минимальным требованиям, он НЕ МОЖЕТ считаться электронным и иметь символ электронного МСОПД. Данный символ РАСПОЛАГАЕТСЯ на лицевой стороне электронного МСОПД предпочтительно в зоне 1. Вышеуказанный символ является позитивом, т. е. темная часть изображения печатается или изображается иным образом. РЕКОМЕНДУЕТСЯ, чтобы символ был хорошо виден и легко распознаваем.

3.2 На рис. II-2 указаны рекомендуемые размеры символа, располагаемого на электронном ПД-2. Его соответствующие размеры составляют: 9,0 мм (0,35 дюйма), 5,25 мм (0,21 дюйма), 3,75 мм (0,15 дюйма), 2,25 мм (0,09 дюйма), 0,75 мм (0,03 дюйма).

3.3 Для электронного ПД-1 РЕКОМЕНДУЕТСЯ использовать пропорционально уменьшенный формат, а именно 4,2 × 7,2 мм (0,17 × 0,28 дюйма).

3.4 Размеры символа МОЖНО пропорционально изменять для использования, например, на фоновой композиции.

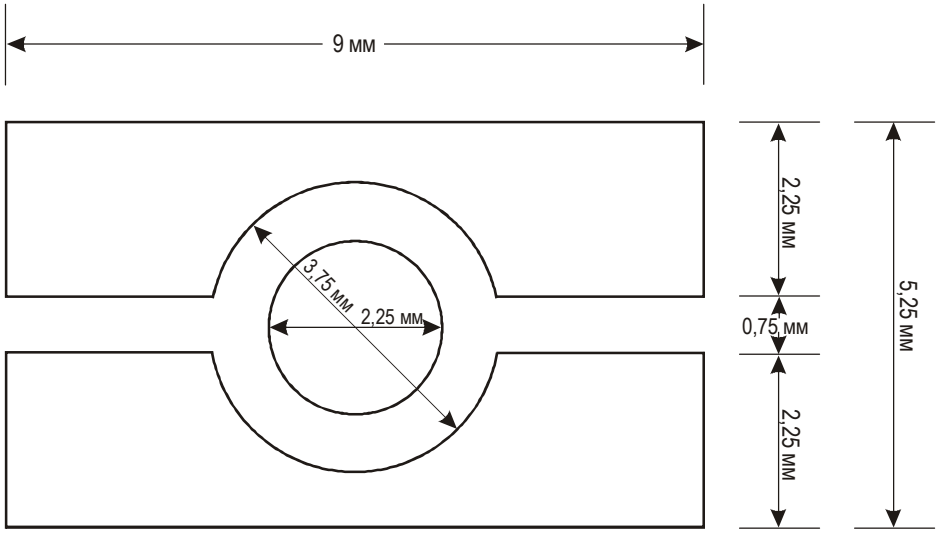


Рис. II-2

4. БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ

4.1 "Биометрическая идентификация" – общий термин, используемый для описания автоматизированных средств распознавания человека путем измерения отличительных физиологических или поведенческих черт.

4.2 "Биометрический шаблон" является автоматически закодированным представлением черты, созданной программно-реализованным алгоритмом; он позволяет производить сравнения (проверки на совпадение) с определенной степенью уверенности в том, что отдельно записанные черты идентифицируют (или не идентифицируют) одного и того же человека. Обычно биометрический шаблон представляет собой относительно небольшой объем данных; однако, поскольку каждый изготовитель биометрической системы использует уникальный формат шаблона, взаимный обмен шаблонами между системами производиться не может. Чтобы государство могло выбрать биометрическую систему, отвечающую его требованиям, данные должны храниться в формате, позволяющем действующей в государстве системе получить шаблон. Это требует обеспечивать хранение биометрических данных в форме одного или нескольких изображений.

4.3 В документе Doc 9303 рассматривается только три вида систем биометрической идентификации. Это физиологические системы:

- распознавания черт лица (обязательное),
- распознавания отпечатка пальца (факультативное),
- распознавания радужной оболочки глаза (факультативное).

Международный стандарт ИСО/МЭК 19794, состоящий из нескольких частей, устанавливает спецификации на эти виды биометрической идентификации. Государства выдачи ОБЕСПЕЧИВАЮТ соответствие этим спецификациям.

4.4 *Биометрические термины.* В контексте биометрической идентификации употребляются следующие термины:

- "верифицировать", т. е. производить проверку на совпадение "один к одному" между представленными биометрическими данными, полученными от владельца МСОПД в настоящий момент, и биометрическим шаблоном, созданным при занесении владельца в систему;

- "идентифицировать", т. е. производить поиск по принципу "один ко многим", сопоставляя представленные биометрические данные с коллекцией шаблонов, представляющих всех субъектов, занесенных в систему.

4.5 При выполнении функции идентификации биометрические параметры могут использоваться для повышения качества проверки анкетных данных в рамках процесса рассмотрения заявлений о выдаче паспорта, визы или иного проездного документа и, кроме того, они могут использоваться для установления точного соответствия между проездным документом и лицом, предъявляющим его.

5. КЛЮЧЕВЫЕ ФАКТОРЫ

При определении выгод использования биометрических данных в МСОПД ключевыми факторами являются:

- *глобальная интероперабельность* – крайняя необходимость установления универсальной интероперабельной системы биометрической идентификации;

- *единообразие* – необходимость максимально возможного сокращения различных вариантов решения, которые потенциально могут применяться государствами-членами, путем установления конкретных стандартов;

- *техническая надежность* – необходимость иметь руководящие принципы и параметры с целью обеспечения использования государствами-членами проверенных технологий, гарантирующих высокую степень уверенности с точки зрения подтверждения личности, а также для того, чтобы государства, считывающие данные, закодированные другими государствами, могли быть уверены в том, что представленные им данные являются достаточно качественными и целостными для проведения точной верификации в своей собственной системе;

- *практическая применимость* – необходимость обеспечения ввода в действие и выполнения рекомендуемых стандартов государствами без использования множества различных систем и технических средств для обеспечения соответствия всем возможным вариантам и интерпретациям стандартов;

- *долговечность* – требование о том, чтобы введенные системы сохранялись в течение максимального десятилетнего срока действия проездного документа, а будущие модификации были совместимы с прежними версиями.

6. КЛЮЧЕВЫЕ ПРОЦЕССЫ В ОТНОШЕНИИ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ

6.1 Основные компоненты биометрической системы:

Установление подлинности личности – несомненное удостоверение подлинности личности зарегистрированного пользователя.
Захват – получение исходного биометрического образца.
Извлечение – преобразование исходных данных биометрического образца в промежуточную форму.
Создание шаблона – преобразование промежуточных данных в шаблон.
Сравнение – сопоставление с информацией в хранящемся контрольном шаблоне.

6.2 Описание соответствующих процессов:

- Процесс *занесения* в систему состоит в захвате исходного биометрического образца. Он используется для взятия биометрических образцов у каждого нового лица (потенциального владельца МСОПД) в целях создания нового шаблона для хранения. Процесс захвата – это автоматическое получение биометрического параметра при помощи таких устройств, как дактилоскопический сканер, сканер для фотографий, цифровая камера прямой съемки или камера, изменяющая масштаб живого изображения радужной оболочки глаза. Для процесса захвата с помощью каждого снимающего устройства должны быть установлены определенные критерии и правила (например, обращение лицом к камере – стандартная поза при съемке для целей

распознавания черт лица; каким образом – нажатием или перекатыванием – следует снимать отпечатки пальцев; глаза должны быть полностью открыты для фиксирования радужной оболочки глаза). Полученное в результате изображение сжимается и затем сохраняется для идентификации личности в будущем.

- В процессе *создания шаблона* сохраняются отличительные и повторяющиеся характеристики взятого биометрического образца, и он обычно осуществляется с помощью собственного программно реализованного алгоритма получения шаблона из хранимого изображения. Это позволяет формировать изображение таким образом, чтобы впоследствии его можно было сравнить с другим образцом изображения, захваченного в тот момент, когда необходимо подтверждать подлинность личности, и дать сравнительную оценку степени совпадения. Неотъемлемым элементом этого алгоритма является контроль качества, благодаря которому посредством определенного механизма оценивается качество образца. Стандарты качества должны быть максимально высокими, так как все будущие проверки будут зависеть от качества первоначально зафиксированного изображения. Если качество является неудовлетворительным, процесс *захвата* следует повторить.

- В процессе *идентификации* берутся шаблоны, полученные на основе новых образцов, и сравниваются с шаблонами зарегистрированных конечных пользователей с целью определить, был ли конечный пользователь ранее зарегистрирован в системе и, если да, является ли он одним и тем же лицом.

- В процессе *верификации* берутся новые образцы владельца электронного МСОПД и сравниваются с ранее записанными шаблонами этого владельца с целью определить, является ли данный владелец одним и тем же лицом.

7. ВИДЫ ПРИМЕНЕНИЯ БИОМЕТРИЧЕСКОГО РЕШЕНИЯ

7.1 Ключевым применением биометрического решения является верификация личности в плане определения связи между владельцем МСОПД и имеющимся у него МСОПД.

7.2 В процессе ввода в систему при обращении за получением МСОПД используется ряд типовых видов применения биометрических параметров.

7.2.1 Биометрические данные конечного пользователя, полученные в процессе занесения в систему, могут использоваться при поиске в одной или нескольких базах биометрических данных (идентификация) с целью установить, известен ли конечный пользователь какой-либо из соответствующих систем (например, как имеющий МСОПД под другим именем, как имеющий криминальное досье, как имеющий МСОПД другого государства).

7.2.2 В момент получения МСОПД конечным пользователем (или его явки на любом этапе процесса выдачи после первоначального обращения за получением паспорта и взятия биометрических данных) его биометрические данные могут быть взяты еще раз и вновь верифицированы путем сопоставления с первоначально взятыми биометрическими данными.

7.2.3 Личность сотрудников, производящих занесение в систему, может верифицироваться для подтверждения того, что они уполномочены на выполнение такой задачи. Это может включать биометрическую аутентификацию для инициализации цифровой подписи в контрольных журналах на различных этапах процесса выдачи, позволяющую с помощью биометрических характеристик устанавливать связь между сотрудниками и действиями, за которые они несут ответственность.

7.3 Имеется также несколько типичных видов применения биометрических параметров на пунктах пограничного контроля.

7.3.1 Всякий раз, когда совершающее поездку лицо (т. е. владелец МСОПД) прибывает в государство или покидает государство, его личность может верифицироваться по изображению, созданному в момент выдачи ему проездного документа. Это гарантирует, что владелец документа является именно тем лицом, которому документ был выдан на законных основаниях, и повышает эффективность любой системы предварительной информации о прибывающих лицах (API). Государство может посчитать нужным хранить биометрический шаблон или шаблоны на проездном документе вместе с изображением, с тем чтобы верификацию лиц, совершающих поездку, можно было производить во внутренних пунктах, где биометрическая система контролируется государством выдачи.

7.3.2 *Двусторонняя проверка*. Взятые текущие биометрические данные пассажира в виде изображения и биометрический шаблон из его проездного документа (или из центральной базы данных) могут проверяться на совпадение с целью подтверждения того, что проездной документ не был изменен.

7.3.3 *Трехсторонняя проверка*. Текущие биометрические данные лица, совершающего поездку, в форме изображения, изображение в его проездном документе и изображение, хранящееся в центральной базе данных, могут проверяться на совпадение (путем построения биометрических шаблонов каждого изображения) с целью подтверждения того, что проездной документ не был изменен. Этим методом проверяется соответствие лица и его МСОПД с базой данных, содержащей данные, внесенные в МСОПД в момент его выдачи.

7.3.4 *Четырехсторонняя проверка*. Четвертая подтверждающая проверка (неэлектронная) представляет собой визуальное сравнение результатов трехсторонней проверки с цифровой фотографией на странице данных МСОПД лица, совершающего поездку.

7.4 Помимо применения биометрических параметров в целях занесения в систему и обеспечения безопасности на границах, демонстрируемого в процессах сравнения "один к одному" и "один ко многим", государствам следует также уделять внимание установлению собственных критериев в отношении:

– точности функций системы, связанных с сопоставлением биометрических данных. Государства выдачи должны кодировать в МСОПД в соответствии со спецификациями LDS один или несколько биометрических параметров лица, отпечатка пальца или радужной оболочки глаза (биометрические параметры могут также храниться в базе данных, доступной принимающему государству). С учетом стандартизированного ИКАО биометрического изображения принимающие государства должны выбрать собственные программные средства биометрической верификации и определить собственные пороговые значения вероятности биометрического определения для установления допустимых отклонений при верификации личности и выявления самозванцев;

– пропускной способности (например, количество пассажиров в минуту) биометрической системы или всей системы контроля за пересечением границы;

– пригодности применения конкретной биометрической технологии (идентификации по лицу, пальцу или глазу) в процессе осуществления контроля за пересечением границы.

8. ОГРАНИЧЕНИЯ В ОТНОШЕНИИ БИОМЕТРИЧЕСКИХ РЕШЕНИЙ

8.1 Общепризнано, что внедрение большинства биометрических технологий зависит от их дальнейшего (быстрого) развития. Принимая во внимание стремительные технологические изменения, любые спецификации (в том числе содержащиеся в этом документе) должны допускать и признавать возможность изменений, связанных с совершенствованием технологий.

8.2 Биометрическая информация, хранящаяся в проездных документах, должна соответствовать всем национальным законам о защите данных или законам о неприкосновенности частной жизни, принятым государством выдачи.

9. ВЗГЛЯД ИКАО НА БИОМЕТРИЧЕСКУЮ ТЕХНОЛОГИЮ

9.1 Концепция ИКАО в части применения биометрической технологии предусматривает:

– спецификацию основной интероперабельной формы биометрической технологии для использования на пунктах пограничного контроля (верификация, списки особого внимания), а также перевозчиками и органами, выдающими документы, и спецификацию согласованных дополнительных биометрических технологий;

– спецификацию биометрических технологий для использования органами, выдающими документы (идентификация, верификация и списки особого внимания);

– способность извлекать данные в течение максимального десятилетнего срока действия, как определено в документе Doc 9303;

– владение несобственническим элементом с целью обеспечения защиты любых государств, вкладывающих средства в биометрию, от меняющихся инфраструктур или поставщиков.

10. ВЫБОР БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ, ПРИМЕНИМЫХ К ЭЛЕКТРОННЫМ МСОПД

10.1 Давно известно, что указание в документе фамилии и репутация честности его предъявителя не гарантируют, что владелец проездного документа (МСОПД), предоставленного ему государством выдачи, является в принимающем государстве тем же лицом, которому был выдан этот документ.

10.2 Единственным методом безоговорочного установления связи человека с его проездным документом является получение его физиологических характеристик, т.е. биометрических признаков человека, владеющего проездным документом, таким способом, который обеспечивает защиту от несанкционированного доступа.

10.3 В результате пятилетнего изучения операционных потребностей в биометрическом идентификаторе, пригодном для использования в процедуре выдачи МСОПД и в различных процессах, связанных с пересечением границ, в соответствии с законами различных государств о неприкосновенности частной жизни, ИКАО определила, что распознавание черт лица должно стать глобально интероперабельной биометрической технологией. В поддержку технологии распознавания черт лица каждое государство факультативно может использовать технологию распознавания отпечатка пальца и/или радужной оболочки глаза.

10.4 Сделав этот вывод, ИКАО отметила, что для большинства государств использование изображения лица человека связано с нижеуказанными преимуществами.

10.4.1 Фотографии с изображением лица не раскрывают информацию, которую человек обычно не раскрывает широкой публике.

10.4.2 Фотография (изображение лица человека) в социальном и культурном отношении уже принята на международном уровне.

10.4.3 Изображение лица уже в обычном порядке используется и верифицируется в рамках процесса обработки заявлений на получение МСОПД с целью изготовления МСОПД в соответствии со стандартами документа Doc 9303.

10.4.4 Широкая общественность уже знакома с процедурой получения изображения лица и использования его для целей верификации личности.

10.4.5 Получение изображения лица не является интрузивной процедурой. Для регистрации конечному пользователю не надо соприкасаться или взаимодействовать с физическим устройством в течение продолжительного времени.

10.4.6 Получение изображения лица не требует введения новых и дорогостоящих процедур занесения в систему.

10.4.7 Технология получения изображения лица может быть задействована практически незамедлительно, причем с возможностью также ретроспективного получения изображения.

10.4.8 Многие государства имеют действующие базы данных с изображениями лица, полученными в рамках изготовления фотографий для проездных документов в цифровой форме, которые могут быть закодированы в шаблоны изображения лица и верифицированы в целях сравнения идентификационной информации.

10.4.9 В соответствующих случаях по решению государства выдачи изображение лица можно снимать с заверенной фотографии без необходимости физического присутствия человека.

10.4.10 Для списков особого внимания фотография с изображением лица обычно является единственным биометрическим параметром, имеющимся для сравнения.

10.4.11 Верификация человеком биометрического параметра путем сравнения с фотографией/ субъектом является относительно простым и известным органам пограничного контроля процессом.

10.5 *Хранение биометрического параметра лица*. Все производители средств распознавания черт лица используют собственные алгоритмы для создания своих биометрических шаблонов. Являясь интеллектуальной собственностью производителей, эти алгоритмы держатся ими в секрете и не могут быть воспроизведены путем обратной инженерии для создания распознаваемого изображения лица. Поэтому шаблоны распознавания черт лица не являются интероперабельными среди производителей, и единственный способ достижения интероперабельности изображения лица состоит в передаче принимающему государству снятой "оригинальной" фотографии. Затем принимающее государство использует алгоритм своего собственного производителя (который может быть или может не быть тем же производителем/вариантом, который используется государством выдачи) для сравнения снятого в реальном времени изображения лица владельца МСОПД с изображением лица, считанным с технического средства хранения данных в МСОПД.

11. ФАКУЛЬТАТИВНЫЕ ДОПОЛНИТЕЛЬНЫЕ БИОМЕТРИЧЕСКИЕ ПАРАМЕТРЫ

11.1 Государства факультативно могут вводить дополнительные данные в свои процессы верификации личности (и процессы других государств) путем включения составной биометрической характеристики в свои проездные документы, т. е. комбинации изображений лица и/или отпечатка пальца и/или радужной оболочки глаза. Это уместно, в частности, там, где государства имеют действующие базы данных отпечатков пальцев и радужных оболочек глаза, в сопоставлении с которыми могут верифицироваться предоставляемые им биометрические параметры, например в рамках системы идентификационных карточек.

11.2 *Хранение факультативного биометрического параметра отпечатка пальца*. Технология биометрической идентификации по отпечаткам пальцев подразделяется на три класса: системы идентификации на основе изображения отпечатка пальца, системы идентификации на основе деталей дактилоскопического узора и системы идентификации на основе дактилоскопической карты. Хотя разработанные стандарты в рамках этих классов делают большинство систем интероперабельными в своем классе, системы, относящиеся к разным классам, интероперабельными не являются. В этой связи появляются три стандарта дактилоскопической интероперабельности: хранение данных изображения, хранение данных детального узора и хранение данных карты. Если государство выдачи решает предоставлять данные отпечатков пальцев в своих электронных МСОПД, хранение изображения отпечатка пальца является обязательным для обеспечения глобальной интероперабельности между классами. Хранение соответствующего шаблона является факультативным и осуществляется по усмотрению государства выдачи.

11.3 *Хранение факультативного биометрического параметра радужной оболочки глаза*. Применение биометрических параметров радужной оболочки глаза осложняется нехваткой испытанных производителей. Фактический стандарт на биометрические параметры радужной оболочки глаза появился на базе методологии одного признанного производителя. Другие производители в будущем могут предложить технологию идентификации по радужной оболочке, однако в качестве отправной точки им, вероятно, потребуется изображение радужной оболочки глаза, а не шаблон, созданный нынешним производителем. Если государство выдачи решает предоставлять данные о радужной оболочке глаза в своих электронных МСОПД, хранение изображения радужной оболочки является обязательным для обеспечения глобальной интероперабельности. Хранение соответствующего шаблона является факультативным и осуществляется по усмотрению государства выдачи.

12. ХРАНЕНИЕ, СЖАТИЕ И ОБРЕЗКА ИЗОБРАЖЕНИЯ

12.1 В структуре LDS элементом данных изменяемого размера, наиболее влияющим на размер LDS, является воспроизводимое изображение. Кроме того, необходимо определять до какого уровня государство выдачи может сжимать изображение без ухудшения результатов биометрического сравнения, проводимого принимающим государством.

12.2 Биометрические системы уменьшают полученное исходное изображение (лицо/отпечаток пальца/радужная оболочка глаза) до размеров признакового пространства, используемого для проверки на совпадение; следовательно, сжатие может производиться с целью уменьшения потребности сохраняемых изображений в памяти при условии, что оно не искажает это признаковое пространство.

12.3 *Размер изображения лица*. Сканирование цветной фотографии стандартного формата ИКАО с разрешающей способностью 300 точек на дюйм дает изображение размером приблизительно 640 кб (килобайт) по 24 бита на пиксель с примерно 90 пикселями между глазами.

Такое изображение можно значительно сжать, используя методику JPEG или JPEG 2000 без существенного ухудшения качества воспринимаемого изображения.

12.4 Проведенные исследования, в которых использовались стандартные фотографии, но с алгоритмами разных производителей и стандартами сжатия JPEG и/или JPEG2000, показали, что *минимальный* практичный размер изображения, подходящий для стандартной фотографии МСОПД ИКАО, составляет приблизительно 12 кб (килобайт). Исследования показали, что степень сжатия сверх этого размера дает значительно менее надежные результаты распознавания черт лица. Емкость в 12 кб не всегда достижима, поскольку при одном и том же коэффициенте сжатия одни изображения компрессируются больше, чем другие, в зависимости от таких факторов, как материал, окраска и прическа. На практике средние размеры сжатого изображения лица в пределах 15–20 кб должны быть оптимальными для использования в электронных МСОПД.

12.4.1 *Обрезка*. Для экономии пространства изображение можно обрезать и показать лишь глаза/нос/рот, однако это существенно снизит способность человека легко удостовериться в том, что данное изображение является изображением того же лица, которое стоит перед ним или фигурирует на фотографии МСОПД.

Например, на рис. II-3 изображение слева намного усложняет задачу распознавания по сравнению с изображением справа.

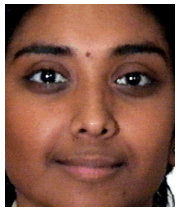


Рис. II-3

Следовательно, изображения, хранящиеся в LDS, РЕКОМЕНДУЕТСЯ:

- либо не обрезать, т. е. делать их идентичными фотографии, напечатанной на МСОПД;
- либо минимально обрезать между подбородком и макушкой и между краями лица, как показано на рис. II-4.

Рис. II-4

12.4.2 Для содействия процессу опознания по лицу изображение лица ХРАНИТСЯ в виде либо полного изображения анфас, либо маркерного изображения в соответствии со спецификациями, установленными стандартом ИСО/МЭК 19794-5 "Информационные технологии. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица". Маркерное изображение – это изображение лица, которое при необходимости поворачивается, с тем чтобы воображаемая горизонтальная линия между центрами глаз была параллельна верхней кромке снимка, размер которого скорректирован. РЕКОМЕНДУЕТСЯ, чтобы расстояние между центрами глаз составляло приблизительно 90 пикселей, как показано на рис. II-5.

Исходное изображение

Маркерное изображение
(наклонено и размер изменен)

Рис. II-5

Логическая структура данных (см. раздел III) может обеспечивать хранение координат положения глаз.

12.4.3 *Лицевые украшения*. Государство выдачи определяет, в какой степени оно будет допускать наличие лицевых украшений на хранящихся (или отображаемых) фотографиях. В общем, если такие украшения носятся постоянно, они могут фигурировать на хранящемся изображении.

12.5 *Размер факультативного изображения отпечатка пальца*. Если государство решает хранить на бесконтактной ИС изображение(я) отпечатков пальцев, то оптимальный размер изображения ДОЛЖЕН составлять приблизительно 10 кб данных на один палец (например, при сжатии типичным методом компрессии WSQ).

12.6 *Размер факультативного изображения радужной оболочки глаза*. Если государство решает хранить на бесконтактной ИС изображение(я) радужной оболочки глаза, то оптимальный размер изображения ДОЛЖЕН составлять приблизительно 30 кб данных на один глаз.

13. ХРАНЕНИЕ БИОМЕТРИЧЕСКИХ И ДРУГИХ ДАННЫХ В ЛОГИЧЕСКОМ ФОРМАТЕ НА БЕСКОНТАКТНОЙ ИС

13.1 ТРЕБУЕТСЯ, чтобы использовались цифровые изображения и чтобы эти изображения хранились в электронном формате в проездном документе.

13.2 Эти изображения должны быть стандартизированы.

13.3 Бесконтактная ИС большой емкости ЯВЛЯЕТСЯ электронным носителем данных, определенным ИКАО в качестве технологии увеличения емкости для применения в электронных МСОПД при использовании средств биометрической идентификации.

13.3.1 *Емкость памяти бесконтактной ИС для хранения данных*. Емкость памяти бесконтактной ИС определяется по усмотрению государства выдачи, но СОСТАВЛЯЕТ как минимум 32 килобайта. Эта минимальная емкость необходима для хранения обязательного изображения лица (обычно 15–20 кб), дубликата данных МСЗ и необходимых элементов защиты данных. Хранение дополнительных изображений лица, отпечатка пальца и/или радужной оболочки глаза, может потребовать значительного увеличения емкости памяти для хранения данных. Максимальная емкость данных бесконтактной ИС не установлена.

13.4 *Хранение других данных*. Любое государство МОЖЕТ использовать емкость памяти бесконтактной ИС электронного МСОПД для увеличения объема машиносчитываемых данных МСОПД сверх уровня, установленного для глобального обмена данными. Это может делаться в таких целях, как предоставление машиносчитываемого доступа к информации исходных документов (например, свидетельства о рождении) и хранящимся данным, используемым для подтверждения личности (биометрические параметры) и/или верификации подлинности документа.

13.5 *Логическая структура данных*. С целью обеспечения глобальной интероперабельности машинного считывания хранящихся данных ДОЛЖНА использоваться логическая структура данных (LDS), определяющая формат записи данных на бесконтактной ИС. Подробное описание LDS приводится в разделе II настоящего тома.

13.6 *Защита и конфиденциальность хранящихся данных*. Как государство выдачи, так и любое принимающее государство должны быть уверены в том, что данные, хранящиеся на бесконтактной ИС, не были изменены со времени их внесения при выдаче документа. Кроме того, законы или практика государства выдачи в отношении неприкосновенности личной жизни могут требовать, чтобы доступ к данным предоставлялся исключительно уполномоченным лицам или организациям. В этой связи ИКАО разработала изложенные в разделе IV спецификации, касающиеся применения и использования современных методов шифрования, в частности интероперабельных схем инфраструктуры открытых ключей (PKI), которые ДОЛЖНЫ использоваться государствами в машиносчитываемых проездных документах, изготовленных в соответствии со спецификациями, изложенными в документе Doc 9303. Основной целью этого является усиление защиты путем применения автоматизированных средств аутентификации МСОПД и их законных владельцев на международном уровне. Кроме того, рекомендуется ряд способов и средств в целях внедрения технологии международной аутентификации электронного МСОПД и указания путей использования электронных МСОПД для упрощения применения биометрии или электронной торговли. Спецификации раздела IV позволяют государству выдачи защищать хранящиеся данные от несанкционированного доступа путем использования средств контроля доступа.

13.7 В настоящих спецификациях указывается, что данные на ИС ЗАПИСЫВАЮТСЯ только во время выдачи МСОПД.

13.8 *PKI*. Основная цель описываемой схемы PKI заключается в том, чтобы позволить полномочным органам, проверяющим электронные МСОПД (в принимающих государствах), производить верификацию аутентичности и целостности данных, хранящихся в электронном МСОПД. Данные спецификации не предписывают полного внедрения сложной структуры PKI, а указывают способ внедрения, при котором государства могут делать выбор в различных сферах (таких, как активная аутентификация, борьба с копированием данных и контроль доступа, автоматизация

процесса пересечения границ и т. д.) и иметь таким образом возможность поэтапно внедрять дополнительные элементы, не противореча всей структуре.

13.8.1 Сертификаты используются в целях безопасности вместе с методологией рассылки открытых ключей (сертификатов) государствам-членам, а инфраструктура приспособлена для достижения целей ИКАО.

13.8.2 Спецификации PKI подробно описываются в разделе IV настоящего тома.

13.9 *PKI и LDS*. В разделах, посвященных LDS и PKI, определяется способ обеспечения целостности и конфиденциальности данных в контексте применения средств биометрической идентификации в МСОПД.

13.10 *Бесконтактная ИС и кодирование.* Бесконтактные ИС, используемые в МСОПД, СООТВЕТСТВУЮТ стандарту ИСО/МЭК 14443 типа A или типа B и стандарту ИСО/МЭК 7816-4. LDS КОДИРУЕТСЯ по методу произвольного доступа. Дальность считывания (достигаемая комбинацией электронного МСОПД и считывающего устройства) должна составлять, как указано в стандарте ИСО/МЭК 14443, до 10 см.

13.11 *Минимум элементов данных, хранящихся в LDS.* Минимумом обязательных элементов данных, подлежащих хранению в LDS на бесконтактной ИС, ЯВЛЯЕТСЯ дубликат данных машиносчитываемой зоны, входящих в группу данных 1, и изображение лица владельца, входящее в группу данных 2. Кроме того, ИС в электронном МСОПД, отвечающем стандартам, СОДЕРЖИТ объект системы защиты (EF.SOD), необходимый для валидации целостности данных, созданных органом выдачи документа; они хранятся в специальном файле № 1, указанном в LDS (см. раздел III). Объект системы защиты (EF.SOD) состоит из используемых хэш-групп данных. Подробная информация содержится в разделе IV.

13.12 *Структура хранящихся данных*. В логической структуре данных, описанной в разделе III, детализируется обязательная и факультативная информация, подлежащая включению в конкретные блоки биометрических данных в рамках LDS.

14. ИЗГОТОВЛЕНИЕ МСОПД И СЧИТЫВАНИЕ ДАННЫХ

14.1 *Изготовление МСОПД.* Технология изготовления, которая обычно используется для изготовления пластиковых карточек, содержащих бесконтактные ИС, вполне пригодна для изготовления МСОПД. Однако, чтобы обеспечить типичный срок службы МСОПД 5–10 лет, необходимо тщательно подбирать материалы, используемые для изготовления таких документов.

14.2 *Считывание данных в формате OCR и данных на бесконтактной ИС.* РЕКОМЕНДУЕТСЯ, чтобы принимающее государство обеспечивало считывание как данных в формате OCR, отпечатанных на МСОПД, так и данных, хранящихся на бесконтактной ИС. В тех случаях, когда государство блокирует бесконтактную ИС в целях защиты от несанкционированного считывания, то для получения доступа к данным на ИС требуется производить считывание в формате OCR. В целях упрощения формальностей желательно использовать только одно считывающее устройство, способное в идеальном случае считывать оба вида данных одновременно. По той причине, что большей частью операции считывания выполняются в пунктах, в которых должно обеспечиваться считывание как МСП, так и МСОПД, государствам следует стремиться к тому, чтобы приобретать считывающие устройства, способные считывать оба типа документов.

15. ПРОЦЕСС СЧИТЫВАНИЯ ЭЛЕКТРОННОГО МСОПД

На рис. II-6 показаны процессы, связанные со считыванием электронного МСОПД до и во время биометрической верификации владельца.

16. ЗАЩИТА ДАННЫХ, ХРАНЯЩИХСЯ НА БЕСКОНТАКТНОЙ ИС

Данные, хранящиеся на бесконтактной ИС, должны быть защищены от изменения. Это означает, что ДОЛЖНА обеспечиваться защита, шифрование и аутентификация данных. Эти концепции подробно излагаются в разделах III (*LDS)* и IV (*PKI*).

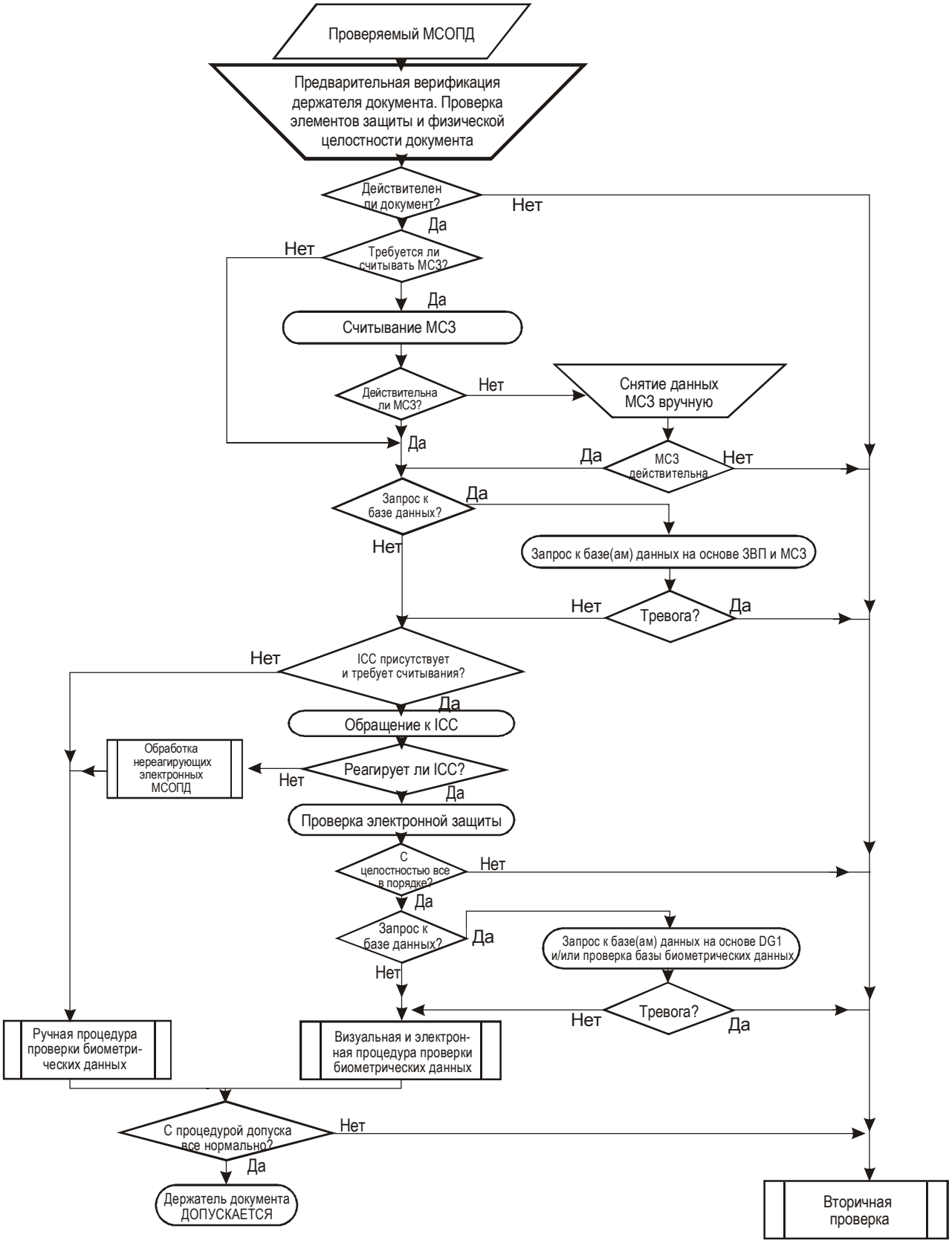

Проверяемый МСОПД
Предварительная верификация держателя документа. Проверка элементов защиты и физической целостности документа
Действителен ли документ?
Нет
Да
Требуется ли считывать МСЗ?
Нет
Да
Считывание МСЗ
Действительна ли МСЗ?
Нет
Снятие данных МСЗ вручную
Да
МСЗ действительна
Да
Нет
Запрос к базе данных?
Да
Нет
Запрос к базе(ам) данных на основе ЗВП и МСЗ
Тревога?
Нет
Да
ICC присутствует и требует считывания?
Нет
Да
Обращение к ICC
Обработка нереагирующих электронных МСОПД
Реагирует ли ICC?
Нет
Да
Проверка электронной защиты
С целостностью все в порядке?
Нет
Да
Запрос к базе данных?
Да
Нет
Запрос к базе(ам) данных на основе DG1 и/или проверка базы биометрических данных
Тревога?
Нет
Да
Ручная процедура проверки биометрических данных
Визуальная и электронная процедура проверки биометрических данных
С процедурой допуска все нормально?
Нет
Да
Держатель документа ДОПУСКАЕТСЯ
Вторичная проверка

Рис. II-6

РАЗДЕЛ III

ЛОГИЧЕСКАЯ СТРУКТУРА ДАННЫХ ДЛЯ ТЕХНОЛОГИИ ХРАНЕНИЯ ДАННЫХ НА БЕСКОНТАКТНОЙ ИНТЕГРАЛЬНОЙ СХЕМЕ

1. СФЕРА ПРИМЕНЕНИЯ

В настоящем разделе описывается логическая структура данных (LDS) электронных МСОПД, необходимая для обеспечения глобальной интероперабельности. Технология увеличения емкости памяти путем использования бесконтактной интегральной схемы, включаемой в МСОПД, если она выбрана государством или организацией выдачи, ДОЛЖНА обеспечивать принимающим государствам доступ к данным. Это требует идентификации всех обязательных и факультативных элементов данных, и, кроме того, должно обеспечиваться нормативное упорядочение и/или группирование данных для достижения глобальной интероперабельности при считывании деталей (элементов данных), записанных на факультативном устройстве увеличения емкости памяти, включенном в МСОПД (электронный МСОПД).

2. СПРАВОЧНЫЕ МАТЕРИАЛЫ

Некоторые положения международных стандартов, на которые делаются ссылки в этом тексте, стали положениями настоящего тома. Эти справочные материалы перечислены в пункте 5 раздела I.

3. ТЕРМИНОЛОГИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Глоссарий терминов, определений и сокращений приводится в начале этого тома.

4. ПОТРЕБНОСТЬ В ЛОГИЧЕСКОЙ СТРУКТУРЕ ДАННЫХ

4.1 Стандартная логическая структура данных (LDS) необходима для обеспечения глобальной интероперабельности при считывании данных, хранящихся на факультативном устройстве увеличения емкости, включаемом в МСПД по усмотрению государства или организации выдачи.

4.2 При разработке LDS ИКАО с самого начала определила в качестве главного требования наличие единой LDS для всех МСПД, использующих любую из рассматриваемых факультативных технологий увеличения емкости памяти. В результате проведенных дискуссий стало очевидно, что бесконтактная интегральная схема является единственной технологией, которая может удовлетворить все потребности ИКАО.

5. ТРЕБОВАНИЯ К ЛОГИЧЕСКОЙ СТРУКТУРЕ ДАННЫХ

5.1 ИКАО установила, что предопределенная стандартная LDS должна отвечать ряду ОБЯЗАТЕЛЬНЫХ требований:

- обеспечивать эффективное и оптимальное упрощение формальностей по отношению к законному владельцу;
- обеспечивать защиту данных, хранящихся на факультативном устройстве увеличения емкости памяти;
- обеспечивать глобальный обмен увеличенными объемами данных на основе использования одной LDS, общей для всех МСПД;
- учитывать различные потребности государств и организаций выдачи в факультативном увеличении объема памяти;
- обеспечивать увеличение емкости памяти по мере роста потребностей пользователей и развития технологии;
- поддерживать разнообразные варианты защиты данных;
- максимально использовать существующие международные стандарты, в частности новые международные стандарты по глобальному обмену интероперабельными биометрическими данными.

6. ОБЯЗАТЕЛЬНЫЕ И ФАКУЛЬТАТИВНЫЕ ЭЛЕМЕНТЫ ДАННЫХ

В целях удовлетворения глобальным требованиям, связанным с оформлением лиц, предъявляющих МСОПД, для LDS определены серии ОБЯЗАТЕЛЬНЫХ и ФАКУЛЬТАТИВНЫХ элементов данных, как это показано на рис. III-1.

7. УПОРЯДОЧЕНИЕ И ГРУППИРОВАНИЕ ЭЛЕМЕНТОВ ДАННЫХ

7.1 Для серии обязательных и факультативных элементов данных установлен логический порядок[1], обеспечиваемый упорядоченными группами взаимосвязанных элементов данных, как это показано на рис. III-1.

7.2 Упорядоченные группы элементов данных затем группируются в зависимости от того, записаны ли они: 1) государством или организацией выдачи или 2) принимающим государством или утвержденной принимающей организацией.

Примечание. Возможность добавления данных к LDS принимающим государством или утвержденной принимающей организацией не обеспечивается LDS, определяемой в настоящем издании части 3 документа Doc 9303.

1. Логический порядок следования элементов данных стандартизирован в соответствии с установленными глобальными требованиями в отношении повышения уровня упрощения формальностей и безопасности при оформлении лиц, предъявляющих МСОПД. Фактический порядок записи сгруппированных элементов данных определяется спецификациями, установленными в целях обеспечения эффективного функционирования устройства увеличения емкости памяти в виде бесконтактной интегральной схемы. Эти спецификации указаны в добавлении 1.

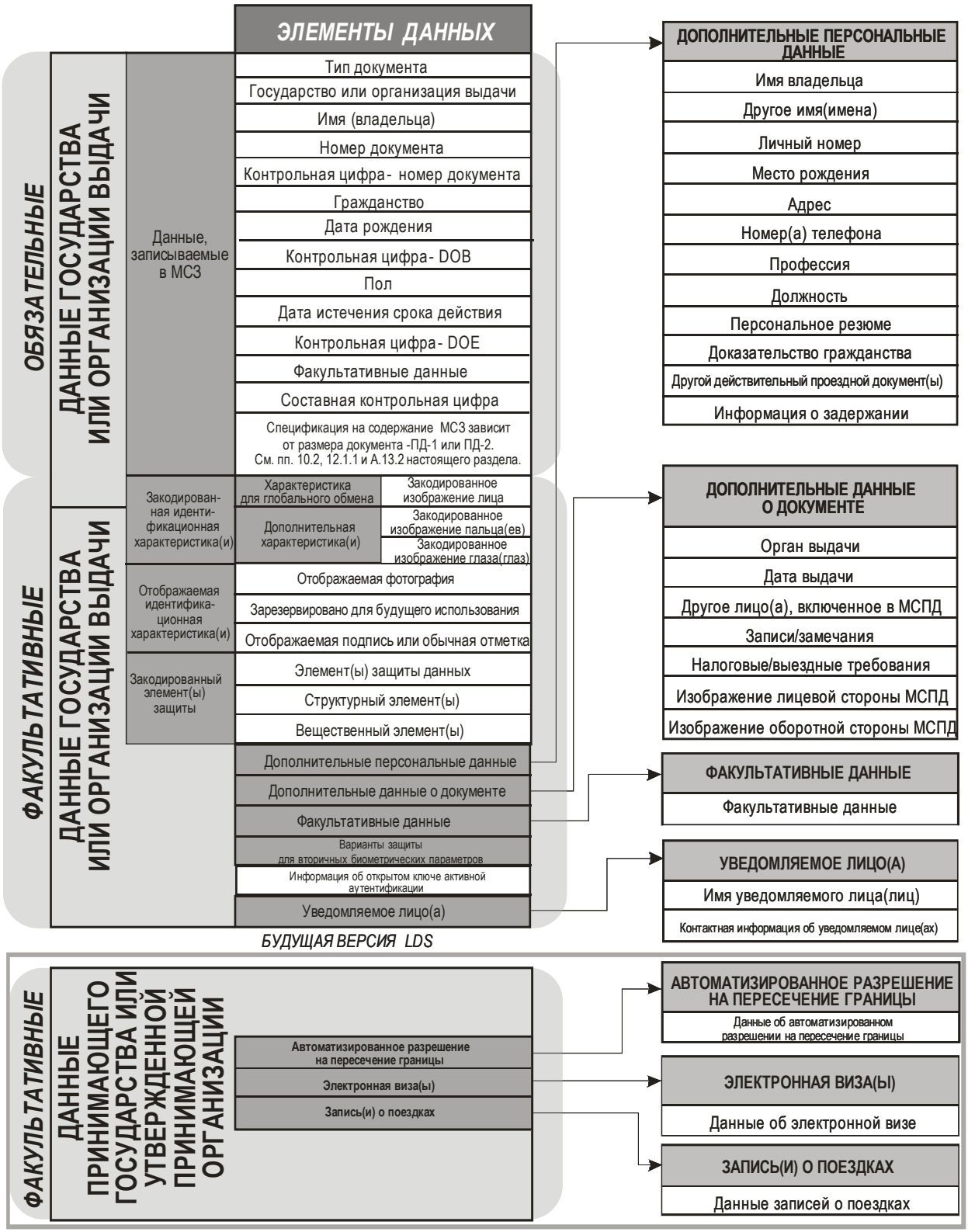


Рис. III-1. Обязательные и факультативные элементы данных, установленные для LDS

7.3 Если LDS записывается на факультативном устройстве увеличения емкости памяти (бесконтактная ИС), то ДОЛЖНЫ включаться четыре группы элементов данных:

- данные, определяющие содержание машиносчитываемой зоны (МСЗ) электронного МСОПД (группа данных 1);
- закодированное изображение лица владельца электронного МСОПД, как определяется в томе 1 и разделе II тома 2 части 3 документа Doc 9303;
- файл EF.COM, содержащий информацию о версии и перечень тегов;
- файл EF.SOD, содержащий информацию о целостности данных и аутентичности.

7.4 Все остальные элементы данных, установленные для записи *государством или организацией выдачи*, являются *факультативными*.

7.5 В LDS могут присутствовать или не присутствовать группы элементов данных, добавляемых *принимающими государствами или утвержденными принимающими организациями*. В LDS может быть несколько записей сгруппированных элементов данных, добавляемых принимающими государствами или утвержденными принимающими организациями.

Примечание. Возможность добавления данных к LDS принимающим государством или утвержденной принимающей организацией не предусматривается в настоящем издании части 3 документа Doc 9303.

7.6 LDS считается единой целостной структурой, содержащей ряд групп элементов данных, записанных на факультативном устройстве увеличения емкости памяти на момент машинного считывания.

Примечание. LDS разработана с достаточной степенью гибкости для применения ее ко всем видам МСПД. Некоторые элементы данных, указанные в последующих таблицах и на рисунках, применимы только к машиносчитываемым визам и машиносчитываемым паспортам, или требуют иной формы представления в данных документах. Эти элементы следует игнорировать в контексте электронных МСОПД.

7.7 В рамках LDS установлены логические группировки соответствующих элементов данных. Эти логические группировки именуются как группы данных.

7.8 Каждой группе данных присваивается ссылочный номер. На рис. III-2 указан ссылочный номер каждой группы; например, "DG2" означает группу данных 2, "закодированная(ые) идентификационная(ые) характеристика(и)" лица законного владельца МСОПД (т. е. биометрические детали лица).

8. ЗАКОДИРОВАННЫЕ ГРУППЫ ДАННЫХ, ПОЗВОЛЯЮЩИЕ ПОДТВЕРДИТЬ АУТЕНТИЧНОСТЬ И ЦЕЛОСТНОСТЬ ДАННЫХ

Для подтверждения аутентичности и целостности записанных данных включается объект аутентичности/целостности. Каждая группа данных ДОЛЖНА быть представлена в этом объекте аутентичности/целостности, который записывается в отдельном элементарном файле (EF.SOD). (См. раздел IV "*PKI*"). Путем использования структуры CBEFF, применяемой для групп данных 2–4 "закодированные идентификационные характеристики" и факультативных "дополнительных элементов биометрической защиты", определяемых в разделе IV *"PKI"*, по решению государства или организации выдачи МОГУТ также отдельно защищаться данные, подтверждающие личность (например, биометрические шаблоны).

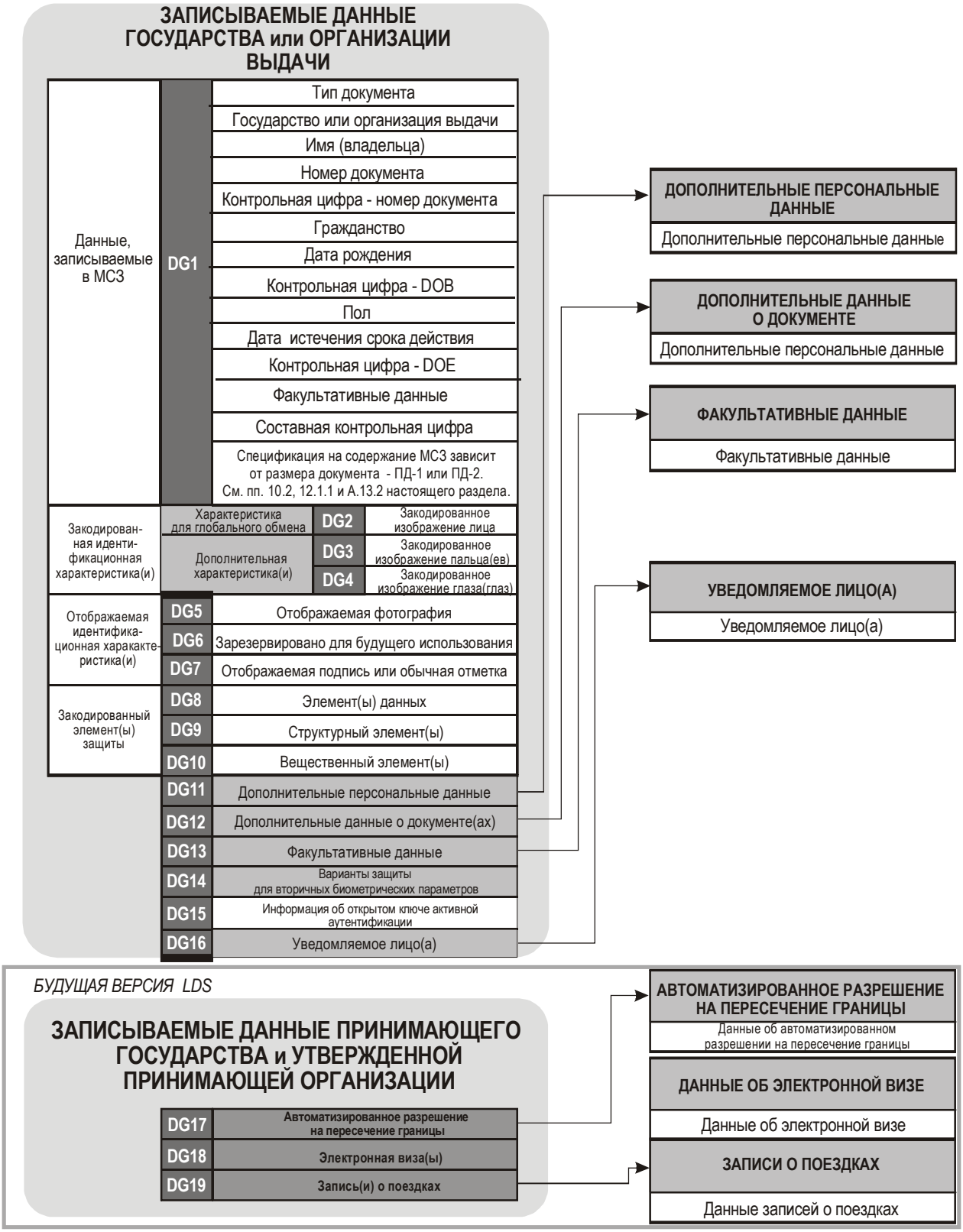


Рис. III-2. Ссылочные номера групп данных в LDS

Примечание к рис. III-2. Вариант добавления принимающим государством данных о разрешении на пересечение границы, электронных визах и поездках (группы данных 17–19) пока не допускается, но, тем не менее, включен в качестве перспективного варианта для использования в будущем.

9. ГРУППЫ ДАННЫХ, ВНОСИМЫХ ГОСУДАРСТВОМ ИЛИ ОРГАНИЗАЦИЕЙ ВЫДАЧИ

В следующей таблице указаны группы данных, которые ДОЛЖНЫ вноситься, и те, которые вносятся ФАКУЛЬТАТИВНО, в совокупности образующие ту часть LDS, которая заполняется государством или организацией выдачи.

Группа данных	**Обязат. (М)/ Факульт. (О)***	**Элемент данных**	
Данные, записываемые в МСЗ МСПД			
1	М	Данные машиносчитываемой зоны (МСЗ)	
Данные машинного подтверждения личности. Закодированная идентификационная (ые) характеристика(и)			
2	М	**ХАРАКТЕРИСТИКА ДЛЯ ГЛОБАЛЬНОГО ОБМЕНА**	Закодированное изображение лица
3	О	Дополнительная характеристика	Закодированное изображение пальца(ев)
4	О	Дополнительная характеристика	Закодированное изображение радужной оболочки глаза (глаз)
Данные машинного подтверждения личности. Отображаемая идентификационная (ые) характеристика(и)			
5	О	Отображаемая фотография *[См. п. 10.4]*	
6	О	Зарезервировано для будущего использования	
7	О	Отображаемая подпись или обычная отметка	
Машинная верификация элементов защиты. Закодированный(е) элемент(ы) защиты			
8	О	Элемент(ы) данных	
9	О	Структурный(е) элемент(ы)	
10	О	Вещественный(е) элемент(ы)	
Дополнительные персональные данные			
11	О	Дополнительные элементы персональных данных	
Дополнительные данные о документе			
12	О	Дополнительные элементы данных о документе	
Факультативные данные			
13	О	Элемент(ы) данных, определяемый(е) по усмотрению государства или организации выдачи	
Зарезервировано			
14	О	Варианты защиты для вторичных параметров	

Группа данных	Обязат. (M)/ Факульт. (O)*	Элемент данных
15	O	Информация об открытом ключе активной аутентификации
Уведомляемое(ые) лицо(а)		
16	O	Элемент(ы) данных об уведомляемом(ых) лице(ах)

* *Редакционное примечание.* "M" означает "mandatory", т. е. обязательные, а "O" – "optional", т. е факультативные.

10. ЭЛЕМЕНТЫ ДАННЫХ, ОБРАЗУЮЩИЕ ГРУППЫ ДАННЫХ 1–16

10.1 Группы данных 1(DG1) – 16 (DG16) в отдельности состоят из ряда обязательных и факультативных элементов данных. В рамках группы данных СОБЛЮДАЕТСЯ установленный порядок последовательности элементов данных.

10.2 В следующих таблицах указаны обязательные и факультативные элементы данных, которые в совокупности образуют структуру групп данных 1 (DG1) – 16 (DG16).

10.2.1 *Данные, вносимые в МСЗ МСОПД.* Ниже приводятся элементы данных, включаемые в группу данных 1 (DG1). Элементы данных DG1 отражают все содержание МСЗ независимо от того, что она содержит – фактические данные или знаки-заполнители. Подробная информация о применении МСЗ содержится в томе 1 части 3 документа Doc 9303, и оно зависит от типа МСОПД (ПД-1 или ПД-2).

Группа данных 1 для МСОПД размера 1 (ПД-1)				
Группа данных	**Номер элемента данных**	**Фиксир. (F)/ перемен. (Var)**	**Обязательный (M)/ факультативный (O)**	**Элемент данных**
DG1			**M**	**МСЗ (Перечень данных, вносимых в МСОПД. См. Том 1 части 3 документа Doc 9303)**
	01	F	M	Код документа
	02	F	M	Организация или государство выдачи
	03	F	M	Номер документа (*Девять наиболее значимых знаков*)
	04	F	M	Контрольная цифра. Номер документа или знак-заполнитель (<), указывающий, что номер документа состоит более чем из девяти знаков.
	05	F	M	Факультативные данные и/или, *если номер документа состоит из более чем девяти знаков*, наименее значимые знаки номера документа плюс контрольная цифра номера документа и знак-заполнитель
	06	F	M	Дата рождения

Группа данных 1 для МСОПД размера 1 (ПД-1)				
Группа данных	**Номер элемента данных**	**Фиксир. (F)/ перемен. (Var)**	**Обязательный (M)/ факультативный (O)**	**Элемент данных**
	07	F	M	Контрольная цифра – дата рождения
	08	F	M	Пол
	09	F	M	Дата истечения срока действия
	10	F	M	Контрольная цифра – дата истечения срока действия
	11	F	M	Гражданство
	12	F	M	Факультативные данные
	13	F	M	Общая контрольная цифра – строки 1 и 2 в МСЗ
	14	F	M	Имя (*владельца*)

Группа данных 1 для МСОПД размера 2 (ПД-2)				
Группа данных	**Номер элемента данных**	**Фиксир. (F)/ перемен. (Var)**	**Обязательный (M)/ факультативный (O)**	**Элемент данных**
DG1			**M**	**МСЗ (Перечень данных, вносимых в МСОПД. См. Том 1 части 3 документа Doc 9303)**
	01	F	M	Код документа
	02	F	M	Организация или государство выдачи
	03	F	M	Имя (*владельца*)
	04	F	M	Номер документа (*девять наиболее значимых знаков*)
	05	F	M	Контрольная цифра. Номер документа или знак-заполнитель (<), указывающий, что номер документа состоит из более чем девяти знаков.
	06	F	M	Гражданство
	07	F	M	Дата рождения
	08	F	M	Контрольная цифра – дата рождения
	09	F	M	Пол
	10	F	M	Дата истечения срока действия
	11	F	M	Контрольная цифра – дата истечения срока действия

Группа данных 1 для МСОПД размера 2 (ПД-2)				
Группа данных	**Номер элемента данных**	**Фиксир. (F)/ перемен. (Var)**	**Обязательный (M)/ факультативный (O)**	**Элемент данных**
	12	F	M	Факультативные данные и/или, *если номер документа состоит из более чем девяти знаков*, наименее значимые знаки номера документа плюс контрольная цифра номера документа и знак-заполнитель
	13	F	M	Составная контрольная цифра – строка 2 в МСЗ

10.2.2 Подробная информация о расчете контрольных цифр приводится в томе 1 части 3 документа Doc 9303.

10.3 *Данные, связанные с машинным подтверждением личности. Закодированная идентификационная(ые) характеристика(и).* В группы данных 2 (DG2) – 4 (DG4) ВКЛЮЧАЮТСЯ следующие элементы данных.

Группа данных	**Номер элемента данных**	**Обязательный (M)/ факультативный (O)**	**Элемент данных**
DG2		**M**	**ИДЕНТИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА ДЛЯ ГЛОБАЛЬНОГО ОБМЕНА. ЛИЦО** *[См. п. 10.3.1]*
	01	M	Количество внесенных закодированных биометрических характеристик лица
	02[2]	M	Заголовок *[см. A1.11.3]*
	03[2]	M	Закодированные биометрические данные лица *[см. A1.11.3]*
ДОПОЛНИТЕЛЬНАЯ(ЫЕ) ИДЕНТИФИКАЦИОННАЯ(ЫЕ) ХАРАКТЕРИСТИКА(И) *[см. п. 10.3.2]*			
DG3		**O**	**ДОПОЛНИТЕЛЬНАЯ ИДЕНТИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА. ПАЛЕЦ (ПАЛЬЦЫ)**
	01	M *(если закодированная характеристика пальца (пальцев) включена)*	Количество внесенных закодированных биометрических характеристик пальца (пальцев)

2. Элемент данных повторяется в группе данных при наличии более одной записи биометрической характеристики, что определяется посредством элемента данных 01. Для конкретного внедрения см. технологическую схему в добавлении 1.

Группа данных	Номер элемента данных	Обязательный (М)/ факультативный (О)	Элемент данных
	02[2]	М *(если закодированная характеристика пальца (пальцев) включена)*	Заголовок *[см. A1.11.3]*
	03[2]	М *(если закодированная характеристика пальца (пальцев) включена)*	Закодированные биометрические данные пальца (пальцев) *[см. A1.11.3]*
DG4		**О**	**ДОПОЛНИТЕЛЬНАЯ ИНДЕНТИФИКАЦИОННАЯ ХАРАКТЕРИСТИКА. РАДУЖНАЯ ОБОЛОЧКА ГЛАЗА (ГЛАЗ)**
	01	М *(если закодированная характеристика глаза (глаз) включена)*	Количество внесенных закодированных характеристик радужной оболочки глаза (глаз)
	02[2]	М *(если закодированная характеристика глаза (глаз) включена)*	Заголовок *[см. A1.11.3]*
	03[2]	М *(если закодированная характеристика глаза (глаз) включена)*	Закодированные биометрические данные радужной оболочки глаза (глаз) *[см. A1.11.3]*

10.3.1 Группа данных 2 (DG2) представляет собой глобально интероперабельный биометрический параметр, используемый для машинного подтверждения личности с помощью машиносчитываемых проездных документов, каковым ЯВЛЯЕТСЯ изображение лица владельца, вводимое в систему распознавания лица. При наличии более одной записи предпочтение отдается самой последней закодированной глобально интероперабельной записи.

10.3.2 ИКАО признает, что в поддержку машинного подтверждения личности государства-члены МОГУТ в дополнение к биометрической технологии использовать технику распознавания отпечатков пальцев и/или радужной оболочки глаза, изображения которых КОДИРУЮТСЯ в рамках группы данных 3 (DG3) и группы данных 4 (DG4) соответственно.

2. Элемент данных повторяется в группе данных при наличии более одной записи биометрической характеристики, что определяется посредством элемента данных 01. Для конкретного внедрения см. технологическую схему в добавлении 1.

10.4 *Данные для машинного подтверждения личности. Отображаемая идентификационная(ые) характеристика(и).* В группы данных 5 (DG5) – 7 (DG7) ВКЛЮЧАЮТСЯ следующие элементы данных.

Группа данных	Номер элемента данных	Обязательный (М)/ факультативный (О)	Элемент данных
DG5		**О**	**ОТОБРАЖАЕМАЯ ФОТОГРАФИЯ**
	01	М *(если вносится отображение фотографии)*	Количество внесенных отображений фотографии
	02[3]	М *(если вносится отображение фотографии)*	Формат(ы) представления отображаемой фотографии *[см. п. 10.4.1]*
DG6		**О**	**Зарезервировано для будущего использования**
DG7		**О**	**ОТОБРАЖЕНИЕ ПОДПИСИ ИЛИ ОБЫЧНОЙ ОТМЕТКИ**
	01	М *(если вносится отображение подписи или обычной отметки)*	Количество отображений подписи или обычных отметок
	02[4]	М *(если вносится отображение подписи или обычной отметки)*	Формат представления отображаемой подписи или обычной отметки *[см. п. 10.4.1]*

10.4.1 Элемент данных 02 группы данных 5 (DG5) и группы данных 7 (DG7) КОДИРУЕТСЯ согласно стандарту ИСО/МЭК 10918: 1994 г. Информационные технологии. Цифровое уплотнение и кодирование неподвижных изображений с непрерывным спектром тонов с использованием варианта JFIF или стандарта ИСО/МЭК 15444. Информационные технологии. Система кодирования изображения JPEG2000.

10.5 *Машинная верификация элементов защиты. Закодированные данные.* В совокупности в группы данных 8 (DG8) – 10 (DG10) ВХОДЯТ следующие элементы данных.

3. Элемент данных повторяется в группе данных при наличии более одной записи биометрической характеристики, что определяется посредством элемента данных 01.

4. Элемент данных повторяется в группе данных при наличии более одной записи биометрической характеристики, что определяется посредством элемента данных 01. Для конкретного внедрения см. технологическую схему в добавлении 1.

Группа данных	Номер элемента данных	Обязательный (М)/ факультативный (О)	Элемент данных
DG8		**О**	**ИНФОРМАЦИННЫЙ(ЫЕ) ЭЛЕМЕНТ(Ы)**
	01	М *(если этот закодированный элемент используется)*	Количество информационных элементов
	02[4]	М *(если этот закодированный элемент используется)*	Заголовок *(подлежит определению)*
	03[4]	М *(если этот закодированный элемент используется)*	Данные об информационном(ых) элементе(ах)
DG9		**О**	**СТРУКТУРНЫЙ(ЫЕ) ЭЛЕМЕНТ(Ы)**
	01	М *(если этот закодированный элемент используется)*	Количество структурных элементов
	02[4]	М *(если этот закодированный элемент используется)*	Заголовок *(подлежит определению)*
	03[4]	М *(если этот закодированный элемент используется)*	Данные о структурном(ых) элементе(ах)
DG10		**О**	**ВЕЩЕСТВЕННЫЙ(Е) ЭЛЕМЕНТ(Ы)**
	01	М *(если этот закодированный элемент используется)*	Количество внесенных вещественных элементов
	02[4]	М *(если этот закодированный элемент используется)*	Заголовок *(подлежит определению)*
	03[4]	М *(если этот закодированный элемент используется)*	Данные о вещественном(ых) элементе(ах)

10.6 *Дополнительные персональные данные.* В совокупности в группу данных 11 (DG11) ВХОДЯТ следующие элементы данных.

4. Элемент данных повторяется в группе данных при наличии более одной записи отображаемой характеристики, что определяется посредством элемента данных 01. Для конкретного внедрения см. технологическую схему в добавлении 1.

Группа данных	Номер элемента данных	Обязательный (М)/ факультативный (О)	Элемент данных
DG11		**О**	**ДОПОЛНИТЕЛЬНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**
	01	О	Имя владельца (основной и вторичный идентификаторы полностью)
	02	О	Другое(ие) имя (имена)
	03	О	Личный номер
	04	О	Место рождения
	05	О	Дата рождения (полностью)
	06	О	Адрес
	07	О	Телефонный(е) номер(а)
	08	О	Профессия
	09	О	Должность
	10	О	Персональное резюме
	11	О	Доказательство гражданства *[см. п. 10.6.1]*
	12	М* ** если элемент данных 13 включен*	Количество других действительных проездных документов
	13	О	Номера других проездных документов
	14	О	Информация о задержании

10.6.1 Элемент данных 11 КОДИРУЕТСЯ в соответствии со стандартом ИСО/МЭК 10918 : 1994. Информационные технологии. Цифровое уплотнение и кодирование неподвижных изображений с непрерывным спектром тонов при использовании формата обмена файлами (JFIF) или стандартом ИСО/МЭК 15444 Информационные технологии. Система кодирования изображения JPEG 2000.

10.7 *Дополнительные данные о документе(ах).* В совокупности в группу данных 12 (DG12) ВХОДЯТ следующие элементы данных.

Группа данных	Номер элемента данных	Обязательный (М)/ факультативный (О)	Элемент данных
DG12			**ДОПОЛНИТЕЛЬНЫЕ ДАННЫЕ О ДОКУМЕНТЕ**
	01	О	Полномочный орган выдачи *(МСОПД)*
	02	О	Дата выдачи *(МСОПД)*
	03	М* ** если другое лицо(а) включено в МСПД*	Количество других лиц в МСОПД *(только МСВ)*
	04	О	Другое(ие) лицо(а), включенное(ые) в МСОПД *(только МСВ)*
	05	О	Подтверждения/замечания *(относящиеся к МСОПД)*
	06	О	Налоговые/выездные требования
	07	О	Изображение лицевой стороны МСОПД *[см. п. 10.7.1]*

Группа данных	Номер элемента данных	Обязательный (M)/ факультативный (O)	Элемент данных
	08	O	Изображение оборотной стороны МСОПД *[см. п. 10.7.1]*
	09	O	Время персонализации МСОПД
	10	O	Машина, использованная для персонализации МСОПД

10.7.1 Элементы данных 07 и 08 КОДИРУЮТСЯ в соответствии со стандартом ИСО/МЭК 10918: 1994. Информационные технологии. Цифровое уплотнение и кодирование неподвижных изображений с непрерывным спектром тонов при использовании формата обмена файлами (JFIF) или стандартом ИСО/МЭК 15444 Информационные технологии. Система кодирования изображения JPEG 2000.

10.8 *Факультативные данные.* В совокупности в группу данных 13 (DG13) ВХОДЯТ следующие элементы данных.

Группа данных	Номер элемента данных	Обязательный (M)/ факультативный (O)	Элемент данных
DG13		**O**	**ФАКУЛЬТАТИВНЫЕ ДАННЫЕ**
	01	M *(Если группа данных 13 включена)*	Данные, определяемые государством или организацией выдачи

10.9 Группа данных 14*:* варианты защиты для вторичных биометрических параметров. Эта группа содержит элементы данных, связанные с защитой таких вторичных биометрических параметров, как отпечаток пальца(ев) и/или радужной оболочки глаза(глаз).

Группа данных	Номер элемента данных	Обязательный (M)/ факультативный (O)	Элемент данных
DG14		**O**	**Варианты защиты для вторичных биометрических параметров**

10.10 Группа данных 15 (DG15): информация об открытом ключе активной аутентификации. Эта группа данных содержит факультативный открытый ключ активной аутентификации (см. раздел IV *PKI*).

Группа данных	Номер элемента данных	Обязательный (M) / факультативный (O)	Элемент данных
DG15		**O**	**Информация об открытом ключе активной аутентификации**

10.11 *Уведомляемое(ые) лицо(а).* В совокупности в группу данных 16 (DG16) ВХОДЯТ следующие элементы данных.

Группа данных	Номер элемента данных	Обязательный (М)/ факультативный (О)	Элемент данных
DG16		**О**	**УВЕДОМЛЯЕМОЕ(ЫЕ) ЛИЦО(А)**
	01	М *(Если группа данных 16 внесена)*	Количество идентифицированных лиц
	02	М *(Если группа данных 16 внесена)*	Внесенные данные о датах
	03	М *(Если группа данных 16 внесена)*	Имя уведомляемого лица
	04	М *(Если группа данных 16 внесена)*	Телефон уведомляемого лица
	05	О	Адрес уведомляемого лица

11. ГРУППЫ ДАННЫХ, ВНОСИМЫХ ПРИНИМАЮЩИМ ГОСУДАРСТВОМ ИЛИ УТВЕРЖДЕННОЙ ПРИНИМАЮЩЕЙ ОРГАНИЗАЦИЕЙ

В следующей таблице указаны факультативные группы данных, образующие в целом ту часть LDS, которая в будущем может стать доступной для внесения данных принимающим государством или утвержденной принимающей организацией.

Примечание. В рамках настоящего издания части 3 документа Doc 9303 принимающему государству или утвержденной принимающей организации не разрешается вносить эти данные. Следовательно, группы данных 17–19 недействительны и в настоящее время не поддерживаются методикой LDS. В этот документ они включены в качестве перспективного варианта для использования в будущем.

Группа данных	Обязательные (М)/факультативные (О)	Элемент данных
Данные, касающиеся автоматизированного разрешения на пересечение границы		
DG17	О	Автоматизированное разрешение на пересечение границы
Электронные визы		
DG18	О	Электронная(ые) виза(ы)
Данные записей о поездках		
DG19	О	Запись(и) о поездках

12. ФОРМАТ ЭЛЕМЕНТОВ ДАННЫХ

12.1 *Директория элементов данных*

В настоящем разделе приводится описание элементов данных, которые могут присутствовать в каждой группе данных.

12.1.1 Элементы данных государства выдачи или утвержденной организации выдачи

Группы данных 1 (DG1) – 16 (DG16). Элементы данных и их формат в каждой группе данных УКАЗАНЫ ниже в таблице:

Примечание. A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак ['<', ' '], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

Элемент данных	Факульт. (O) или обязат. (M)	Название элемента данных	Коли-чество байтов	Фиксир. (F) или перемен. (Var)	Тип кодиро-вания	Требования к кодированию
ГРУППА ДАННЫХ 1. Данные, вносимые в МСЗ						
МСОПД размера 1 (ПД-1)						
01	M	Код документа	2	F	A,S	Тип документа (согласно МСЗ в томе 1, A . . . .Z и <)
02	M	Государство или организация выдачи	3	F	A,S	Государство или организация выдачи (согласно МСЗ в томе 1, A . . . .Z и <)
03	M	Номер документа	9	F	A,N,S	Номер документа (согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <) Примечание. Если номер документа состоит более чем из девяти знаков, на позиции контрольной цифры (DE 05) ставится знак-заполнитель (<), а остальные знаки, составляющие номер документа, вносятся в начале DE 12, после чего следуют контрольная цифра номера документа и знак-заполнитель (<)
04	M	Контрольная цифра – *Номер документа*	1	F	N,S	Контрольная цифра элемента данных 03 (согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <)
05	M *Если в МСЗ вносятся факультативные данные*	Факультативные данные	15	F	A, N,S	Согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <
06	M	Дата рождения	6	F	N,S	Формат = YYMMDD согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <. Полная дата рождения (DOB) может храниться в DG11 в формате CCYYMMDD во избежание неясности в кодировании года
07	M	Контрольная цифра – *Дата рождения*	1	F	N	Контрольная цифра элемента данных 06 (согласно МСЗ в томе 1)
08	M	Пол	1	F	A,S	Согласно МСЗ в томе 1, A . . . .Z и <
09	M	Дата истечения срока действия	6	F	N	Формат = YYMMDD согласно МСЗ в томе 1

Элемент данных	Факульт. (O) или обязат. (M)	Название элемента данных	Коли-чество байтов	Фиксир. (F) или перемен. (Var)	Тип кодиро-вания	Требования к кодированию
10	M	Контрольная цифра – *Дата истечения срока действия*	1	F	N	Контрольная цифра элемента данных 09 (согласно МСЗ в томе 1)
11	M	Гражданство	3	F	A,S	Трехбуквенный код (согласно МСЗ в томе 1, A . . . .Z и <)
12	*M Если в МСЗ есть факультативные данные*	*Факультативные данные*	11	F	A,N,S	Согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <
13	M	Контрольная цифра – *Общая контрольная цифра*	1	F	N	Согласно МСЗ в томе 1
14	M	Имя владельца *(первичный и вторичный идентификаторы)*	30	F	A,S	A . . . .Z и <; один или два знака заполнителя (<), вносимые согласно МСЗ в томе 1
МСОПД размера 2 (ПД-2)						
01	M	Код документа	2	F	A,S	Тип документа (согласно МСЗ в томе 1, A . . . .Z и <)
02	M	Государство или организация выдачи	3	F	A,S	Государство или организация выдачи (согласно МСЗ в томе 1, A . . . .Z и <)
03	M	Имя владельца *(первичный и вторичный идентификаторы)*	31	F	A,S	A . . . .Z и <; один или два знака заполнителя (<), вносимые согласно МСЗ в томе 1
04	M	Номер документа	9	F	A,N,S	Номер документа (согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <) Примечание. Если номер документа состоит более чем из девяти знаков, на позиции контрольной цифры (DE 05) ставится знак-заполнитель (<), а остальные знаки, составляющие номер документа, вносятся в начале DE 12, после чего следуют контрольная цифра номера документа и знак-заполнитель (<)
05	M	Контрольная цифра – *Номер документа*	1	F	N,S	Контрольная цифра элемента данных 04 (согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <)

Элемент данных	Факульт. (O) или обязат. (M)	Название элемента данных	Коли-чество байтов	Фиксир. (F) или перемен. (Var)	Тип кодиро-вания	Требования к кодированию
06	M	Гражданство	3	F	A,S	Трехбуквенный код (согласно МСЗ в томе 1, A . . . .Z и <)
07	M	Дата рождения	6	F	N,S	Формат = YYMMDD согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <. Полная дата рождения (DOB) может храниться в DG11 в формате CCYYMMDD во избежание неясности в кодировании года
08	M	Контрольная цифра – *Дата рождения*	1	F	N	Контрольная цифра элемента данных 07 (согласно МСЗ в томе 1)
09	M	Пол	1	F	A,S	Согласно МСЗ в томе 1, A . . . .Z и <
10	M	Дата истечения срока действия	6	F	N	Формат = YYMMDD согласно МСЗ в томе 1
11	M	Контрольная цифра – *Дата истечения срока действия*	1	F	N	Контрольная цифра элемента данных 10 (согласно МСЗ в томе 1)
12	M *Если в МСЗ есть факуль-тативные данные*	*Факультативные данные*	7	F	A,N,S	Согласно МСЗ в томе 1, A. . . Z, 0 . . . 9 и <
13	M	Контрольная цифра – *составная контрольная цифра*	1	F	N	Согласно МСЗ в томе 1
ГРУППА ДАННЫХ 2. Закодированные идентификационные характеристики: ЛИЦО						
01	M	Количество вне-сенных кодиро-вок биометричес-ких характери-стик лица	1	F	N	Цифры 1–9, указывающие количество уникальных кодировок данных о лице
02	M	Заголовок		F		Подробная информация о кодировании содержится в *Нормативном добавлении 1 (A1.11.3)*. Элемент данных может повторяться, как определено DE 01
03	M	Кодировка(и) биометрических характеристик лица	99999 Макс.	Var	A,N,S,B	Подробная информация о кодировании содержится в *Нормативном добавлении 1 (A1.11.3)*. Элемент данных может повторяться, как определено DE 01

Элемент данных	Факульт. (O) или обязат. (M)	Название элемента данных	Коли-чество байтов	Фиксир. (F) или перемен. (Var)	Тип кодиро-вания	Требования к кодированию
ГРУППА ДАННЫХ 3. Закодированные идентификационные характеристики: ПАЛЕЦ (ПАЛЬЦЫ)						
01	M *Если закодированная характеристика пальца (пальцев) включена*	Количество внесенных кодировок биометрических характеристик пальца	1	F	N	Цифры 1–9, указывающие количество индивидуальных кодировок данных о пальце (пальцах)
02	M *Если закодированная характеристика пальца (пальцев) включена*	Заголовок		F		Подробная информация о кодировании содержится в *Нормативном добавлении 1 (A1.13.3)*. Элемент данных может повторяться, как определено DE 01
03	M *Если закодированная характеристика пальца (пальцев) включена*	Кодировка(и) биометрических данных о пальце	99999 Макс.	Var	A,N,S,B	Подробная информация о кодировании содержится в *Нормативном добавлении 1*. Элемент данных может повторяться, как определено DE 01
ГРУППА ДАННЫХ 4. Закодированные идентификационные характеристики: РАДУЖНАЯ ОБОЛОЧКА ГЛАЗА (ГЛАЗ)						
01	M *Если закодированная характеристика глаза (глаз) включена*	Количество внесенных кодировок биометрических характеристик глаза	1	F	N	Цифры 1–9, указывающие количество уникальных кодировок данных о глазе (глазах)
02	M *Если закодированная характеристика глаза (глаз) включена*	Заголовок		F		Подробная информация о кодировании содержится в *Нормативном добавлении 1*. Элемент данных может повторяться, как определено DE 01
03	M *Если закодированная характеристика глаза (глаз) включена*	Кодировка(и) биометрических данных о глазе	99999 Макс.	Var	A,N,S,B	Подробная информация о кодировании содержится в *Нормативном добавлении 1*. Элемент данных может повторяться, как определено DE 01

Элемент данных	Факульт. (O) или обязат. (M)	Название элемента данных	Коли-чество байтов	Фиксир. (F) или перемен. (Var)	Тип кодиро-вания	Требования к кодированию
ГРУППА ДАННЫХ 5. Отображаемая идентификационная характеристика(и): ФОТОГРАФИЯ						
01	M *Если отобра-жаемая фотография включена*	Количество записей: отображаемая фотография	1	F	N	Цифры 1–9, указывающие количество индивидуальных записей отображаемой фотографии
02	M *Если отобра-жаемая фотография включена*	Данные об отображаемой фотографии		F		Элемент данных может повторяться, как определено DE 01
	M Если отобра-жаемая фотография включена	*Количество байтов в представлении отображаемой фотографии*	5	F	N	Цифры 00001–99999, указывающие количество байтов в представлении отображаемой фотографии
	M Если отобра-жаемая фотография включена	*Представление отображаемой фотографии*	99999 Макс.	Var	A,N,S,B	Форматируется согласно ИСО/МЭК 10918-1 или ИСО/МЭК 15444
ГРУППА ДАННЫХ 6. Зарезервировано для будущего использования						
ГРУППА ДАННЫХ 7. Отображаемые идентификационные характеристики: ПОДПИСЬ или ОБЫЧНАЯ ОТМЕТКА						
01	M *Если отобра-жаемая подпись или обычная отметка включена*	Количество записей: отображаемая подпись или обычная отметка	1	F	N	Цифры 1–9, указывающие количество индивидуальных записей отображаемой подписи или обычной отметки
02	M *Если ото-бражаемая подпись или обычная отметка включена*	Данные об отображаемой подписи или обычной отметке	99999 Макс.	Var	A,N,S,B	Элемент данных может повторяться, как определено DE 01. Форматируется согласно ИСО/МЭК 10918-1 или ИСО/МЭК 15444
ГРУППА ДАННЫХ 8. Закодированные элементы защиты: ИНФОРМАЦИОННЫЙ(Е) ЭЛЕМЕНТ(Ы)						
01	M *Если зако-дированный информа-ционный элемент включен*	Количество информационных элементов	1	F	N	Цифры 1–9, указывающие количество индивидуальных записей информационных элементов (охватывает элементы с DE 02 по DE 04)

Элемент данных	Факульт. (O) или обязат. (M)	Название элемента данных	Коли-чество байтов	Фиксир. (F) или перемен. (Var)	Тип кодиро-вания	Требования к кодированию
02	M *Если закодированный информационный элемент включен*	Информация о заголовке	1	TBD		Определяются детали заголовка
03	*M Если закодированный информационный элемент включен*	Данные об информационном элементе	999 Макс.	Var	A,N,S,B	Формат определяется по усмотрению государства или организации выдачи
ГРУППА ДАННЫХ 9. Закодированные элементы защиты: СТРУКТУРНЫЙ(Е) ЭЛЕМЕНТ(Ы)						
01	M *Если закодированный структурный элемент включен*	Количество структурных элементов	1	F	N	Цифры 1–9, указывающие количество уникальных закодированных структурных элементов (охватывает элементы с DE 02 по DE 04)
02	M *Если закодированный структурный элемент включен*	Информация о заголовке	TBD	TBD	N	Определяются детали заголовка
03	*M Если закодированный структурный элемент включен*	Данные о структурном элементе	999 Макс.	Var	A,N,S,B	Формат определяется по усмотрению государства или организации выдачи
ГРУППА ДАННЫХ 10. Закодированные элементы защиты: ВЕЩЕСТВЕННЫЙ(Е) ЭЛЕМЕНТ(Ы)						
01	M *Если закодированный вещественный элемент включен*	Количество вещественных элементов	1	F	N	Цифры 1–9, указывающие количество уникальных закодированных вещественных элементов (охватывает элементы с DE 02 по DE 04)
02	M *Если закодированный вещественный элемент включен*	Информация о заголовке	TBD	TBD	N	Определяются детали заголовка

Элемент данных	Факульт. (O) или обязат. (M)	Название элемента данных	Коли-чество байтов	Фиксир. (F) или перемен. (Var)	Тип кодиро-вания	Требования к кодированию
03	*M Если зако-дированный веществен-ный элемент включен*	Данные о вещественном элементе	999 Макс.	Var	A,N,S,B	Формат определяется по усмотрению государства или организации выдачи
ГРУППА ДАННЫХ 11. Дополнительные персональные данные						
См. директорию элементов данных: дополнительные персональные данные [см. п. 12.1.2]						
ГРУППА ДАННЫХ 12. Дополнительные данные о документе						
См. директорию элементов данных: дополнительные данные о документе [см. п. 12.1.3]						
ГРУППА ДАННЫХ 13. Факультативные данные						
См. директорию элементов данных: факультативные данные [см. п. 12.1.4]						
ГРУППА ДАННЫХ 14. Варианты защиты для вторичных биометрических параметров						
Зарезервировано						
ГРУППА ДАННЫХ 15. Информация об открытом ключе активной аутентификации						
Информация об открытом ключе активной аутентификации приводится в разделе IV настоящего тома "PKI для машиносчитываемых проездных документов с доступом к ICC только для считывания"						
ГРУППА ДАННЫХ 16. Уведомляемое(ые) лицо(а)						
См. директорию элементов данных: данные об уведомляемом(ых) лице(ах) [см. п. 12.1.5]						

12.1.2 *Группа данных 11 (DG11)*. Элементы данных и их формат в **DG11 "Дополнительные персональные данные"** УКАЗАНЫ ниже в таблице.

Примечание. A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак ['<' ' '], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

ГРУППА ДАННЫХ 11. Дополнительные персональные данные						
Элемент данных	**Факульт. (O) или обязат. (M)**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. (F) или перемен. (Var)**	**Тип кодиро-вания**	**Требования к кодированию**
01		Имя владельца (полностью)	99 Макс.	Var	A,B,S	Знаки-заполнители (<) ставятся согласно MC3. В конце строки заполни-тели не ставятся. Сокра-щение не допускается
02	O	Другое(ие) имя (имена)	99 Макс.	Var	A,B,S	Знаки-заполнители (<) ставятся согласно MC3. В конце строки заполни-тели не ставятся. Сокра-щение не допускается
03	O	Личный номер	99 Макс.	Var	A,N,S	Текст произвольного формата
04	O	Место рождения	99 Макс.	Var	A,N,S,B	Текст произвольного формата

ГРУППА ДАННЫХ 11. Дополнительные персональные данные						
Элемент данных	**Факульт. (O) или обязат. (M)**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. (F) или перемен. (Var)**	**Тип кодиро-вания**	**Требования к кодированию**
05	O	Адрес	99 Макс.	Var	A,N,S,B	Текст произвольного формата
06	O	Полная дата рождения	8	F	N	CCYYMMDD
07	O	Телефон	99 Макс.	Var	N,S	Текст произвольного формата
08	O	Профессия	99 Макс.	Var	A,N,S,B	Текст произвольного формата
09	*M, если DE 08 включен*	Должность	99 Макс.	Var	A,N,S,B	Текст произвольного формата
10	*M, если DE 09 включен*	Персональное резюме	99 Макс.	Var	A,N,S,B	Текст произвольного формата
11	*M, если DE 10 включен*	Доказательство гражданства	9999999 Макс.	Var	A,N,S,B	Изображение документа о гражданстве форматируется согласно ИСО/МЭК 10918-1
12	O	Другой действитель-ный(ые) проездной(ые) документ(ы) *Номер проездного документа*	99 Макс.	Var	A,N,S,B	Текст произвольного формата, отделяемый знаком <
13	O	Информация о задержании	999 Макс.	Var	A,N,S,B	Текст произвольного формата

12.1.3 *Группа данных 12 (DG12).* Элементы данных и их формат в **DG12 "Дополнительные данные о документе"** УКАЗАНЫ ниже в таблице.

Примечание. A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак ['<' ' '], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

ГРУППА ДАННЫХ 12. Дополнительные данные о документе						
Элемент данных	**Факульт. (O) или обязат. (M)**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. (F) или перемен. (Var)**	**Тип кодиро-вания**	**Требования к кодированию**
01	O	Полномочный орган выдачи	99 Макс.	Var	A,N,S	Текст произвольного формата
02	O	Дата выдачи	8	F	N	Дата выдачи документа, т. е. YYYYMMDD
03	O	Данные о другом(их) лице(ах)	99 Макс.	Var	A,N,S	Текст произвольного формата (действителен только с МСВ)

ГРУППА ДАННЫХ 12. Дополнительные данные о документе						
Элемент данных	**Факульт. (O) или обязат. (M)**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. (F) или перемен. (Var)**	**Тип кодиро-вания**	**Требования к кодированию**
04	O	Подтверждение(я)/ замечание(я)	99 Макс	Var	A,N,S	Текст произвольного формата
05	O	Налоговые/выездные требования	99 Макс.	Var	A,N,S	Текст произвольного формата
06	O	Изображение лицевой стороны МСОПД	9999999 Макс.	Var	A,N,S,B	Форматируется согласно ИСО/МЭК 10918-1
07	O	Изображение оборотной стороны МСОПД	9999999 Макс.	Var	A,N,S,B	Форматируется согласно ИСО/МЭК 10918-1
08	O	Время персонализации	14	F	N	ccyymmddhhmmss
09	O	Серийный номер устройства персонализации	99 Макс.	Var	A,N,S	Произвольный формат

12.1.4 *Группа данных 13 (DG13).* Элементы данных и их формат в **DG13 "Факультативные данные"** УКАЗАНЫ ниже в таблице.

Примечание. A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак ['<' ' '], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

ГРУППА ДАННЫХ 13. Факультативные данные						
Элемент данных	**Факульт. (O) или обязат. (M)**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир. (F) или перемен. (Var)**	**Тип кодиро-вания**	**Требования к кодированию**
TBD	O	Факультативные данные		Var		По усмотрению государства или организации выдачи

12.1.5 *Группа данных 16 (DG16).* Элементы данных и их формат в **DG16 "Уведомляемое(ые) лицо(а)"** УКАЗАНЫ ниже в таблице.

Примечание. A – буквенный знак [a..z, A..Z], N – цифровой знак [0..9], S – специальный знак ['<' ' '], B – 8-битные двоичные данные (любые, кроме A, N или S), F – поле фиксированной длины, Var – поле переменной длины.

ГРУППА ДАННЫХ 16. Уведомляемое(ые) лицо(а)						
Элемент данных	**Факульт. (O) или обязат. (M)**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир.(F) или перемен. (Var)**	**Тип кодиро-вания**	**Требования к кодированию**
01	M, *если DG 16 включена*	Количество идентифицируемых лиц	2	F	N	Указывает количество лиц, включенных в эту группу данных
02	M, *если DG 16 включена*	Внесенные данные о дате	8	F	N	Внесенная дата уведомления; формат – CCYYMMDD

ГРУППА ДАННЫХ 16. Уведомляемое(ые) лицо(а)						
Элемент данных	**Факульт. (O) или обязат. (M)**	**Название элемента данных**	**Коли-чество байтов**	**Фиксир.(F) или перемен. (Var)**	**Тип кодиро-вания**	**Требования к кодированию**
03	M, *если DG 16 включена*	Имя уведомляемого лица. *Основной и вторичный идентификаторы*		Var	A,S	Знаки-заполнители (<) вносятся согласно МСЗ. Сокращение не допускается
04	M, *если DE 03 включен*	Номер телефона уведомляемого лица		Var	N,S	Номер телефона в международной форме (код страны и местный номер)
05	M	Адрес уведомля-емого лица		Var	A,N,S	Текст произвольного формата

13. ПРИНЦИПЫ БЕЗОПАСНОСТИ

Дополнительная информация о принципах безопасности, применяемых для защиты записанной логической структуры данных (LDS) и обеспечения возможности подтверждения принимающим государством или утвержденной принимающей организацией аутентичности и целостности данных, считываемых с факультативного устройства увеличения емкости памяти, содержится в разделе IV "*PKI*".

14. ПРИНЦИПЫ ОТОБРАЖЕНИЯ ПРИМЕНИТЕЛЬНО К ТЕХНОЛОГИИ РАСШИРЕНИЯ ЕМКОСТИ ДАННЫХ НА БЕСКОНТАКТНОЙ ИС

14.1 *Упорядочение LDS*. Только схема произвольного упорядочения ОБЕСПЕЧИВАЕТ международную интероперабельность. Она описывается в добавлении 1 (нормативное) к настоящему разделу.

14.2 *Схема произвольного упорядочения.* Схема произвольного упорядочения позволяет записывать группы данных и элементы данных, следуя произвольному порядку в соответствии со способностью факультативной технологии увеличения емкости, обеспечивать прямое извлечение конкретных элементов данных даже в случае их беспорядочной записи. Элементы данных переменной длины кодируются как *значения длины,* и длина указывается в нотации ASN.1.

15. ИНФОРМАЦИЯ О ЗАГОЛОВКЕ И ПРИСУТСТВИИ ГРУПП ДАННЫХ

15.1 Карта отображения заголовка и присутствия групп данных ВКЛЮЧЕНА. Эта информация хранится в EF.COM. См. добавление 1.

Рис. III-3. Информация об обязательном заголовке и присутствии групп данных

15.1.1 *Заголовок.* Заголовок СОДЕРЖИТ указанную ниже информацию, позволяющую принимающему государству или утвержденной принимающей организации локализовать и декодировать различные группы данных и элементы данных, содержащиеся в блоке данных, записанном государством или организацией выдачи.

ИДЕНТИФИКАТОР ПРИЛОЖЕНИЯ (AID)
НОМЕР ВЕРСИИ LDS
НОМЕР ВЕРСИИ UNICODE

15.1.2 *Номер версии LDS.* Номер версии LDS определяет версию формата LDS[5]. Точный формат, подлежащий использованию для хранения этого значения, будет определен в добавлении, касающемся технологии отображения. Стандартным форматором номера версии LDS является "aabb", где:

"aa" – число (01–99), идентифицирующее версию LDS (т. е. существенное добавление к LDS);

"bb" – число (01-99), идентифицирующее модификацию LDS.

15.1.3 *Номер версии Unicode*[6]. Номер версии Unicode определяет применяемый метод кодирования при записи буквенных, цифровых и специальных знаков, включая национальные знаки. Точный формат, подлежащий использованию для хранения этого значения, будет определен в добавлении, касающемся технологии отображения. Стандартным форматом номера версии Unicode является "aabbcc", где:

"aa" – число, идентифицирующее **основную версию** стандарта Unicode (т. е. значительные добавления к стандарту, опубликованные в виде справочника);

"bb" – число, идентифицирующее **вспомогательную версию** стандарта Unicode (т. е добавления к знакам или более существенные нормативные изменения, опубликованные в виде **технического** доклада);

"cc" – номер, идентифицирующий **новую версию** стандарта Unicode (т. е. любые другие изменения нормативных или важных информативных частей данного стандарта, которые могут изменить режим

5. Предполагается, что в будущем стандартная организация LDS будет модифицироваться; такие модификации будут рассматриваться в публикуемых поправках к спецификациям ИКАО. Каждой модификации будет присваиваться номер версии, с тем чтобы принимающие государства и утвержденные принимающие организации могли точно декодировать все версии LDS.

6. *Unicode* базируется на ИСО/МЭК 10646. Подробная информация о *Unicode* содержится на сайте www.unicode.org.

работы программы. Эти изменения отражаются в новых файлах символьной базы данных Unicode и на странице обновления).

Примечание. Исторически сложилось так, что нумерация внутри каждого поля (т. е. a, b, c) не обязательно является последовательной.

15.2 *Карта отображения присутствия групп данных.* Карта отображения присутствия групп данных (DGPM) содержит информацию, позволяющую принимающему государству или утвержденной принимающей организации определять, какие группы данных присутствуют в блоке данных, внесенных государством или организацией выдачи.

15.2.1 DGPM, используемая при внедрении интегральных схем, СОСТОИТ из списка "тегов" согласно правилам идентификации элементов данных, записанных на контактной(ых) и бесконтактной(ых) интегральной(ых) схеме(ах), в котором каждый тег указывает, записана ли конкретная группа данных в блоке данных, записанных государством или организацией выдачи. Эта DGPM реализуется как список тегов; тег = '5C' в EF.COM. См. добавление 1.

Группа данных "n" ТЕГ

•
•

Группа данных "m" ТЕГ

Присутствие ТЕГа = Группа данных присутствует.
Отсутствие ТЕГа = Группа данных отсутствует.

15.3 *Карты отображения присутствия элементов данных.* Аналогичная концепция карт отображения присутствия используется применительно к ряду групп данных, содержащих серию подчиненных элементов данных, которые могут включаться по усмотрению государства или организации, делающих запись. Эти карты отображения присутствия, именуемые картами отображения присутствия элементов данных (DEPM), размещаются в начале этих конкретных групп данных, допускающих факультативное расширение объема данных, как иллюстрируется на рис. III-4.

Группы данных, требующие использования карты отображения присутствия элементов данных, определяются в нормативном добавлении 1.

Рис. III-4. Карта отображения присутствия элементов данных

15.3.1 DEPM СОДЕРЖИТ информацию, позволяющую принимающему государству или утвержденной принимающей организации определить, какие элементы данных присутствуют в группе данных.

15.3.2 DEPM состоит из списка "ТЕГов" согласно правилам идентификации элементов данных, записанных на контактной(ых) и бесконтактной(ых) интегральной(ых) схеме(ах), в котором каждый тег указывает, записан ли конкретный элемент данных в группе данных. Эта форма DEPM кодируется как список тегов в соответствующей группе данных.

Присутствие ТЕГа = Элемент данных присутствует.
Отсутствие ТЕГа = Элемент данных отсутствует.

Примечание. Количество байтов, выделяемых для DEPM, определяется в нормативном добавлении 1 к разделу III.

Добавление 1 (НОРМАТИВНОЕ) к разделу III

ОТОБРАЖЕНИЕ LDS НА БЕСКОНТАКТНЫХ ИНТЕГРАЛЬНЫХ СХЕМАХ (ИС) С ИСПОЛЬЗОВАНИЕМ МЕТОДА ПРЕДСТАВЛЕНИЯ ДАННЫХ ПУТЕМ ПРОИЗВОЛЬНОГО ДОСТУПА

A1.1 *Сфера применения.* В добавлении 1 определяются текущие спецификации, регулирующие отображение логической структуры данных – LDS [версия 1.7] на интегральных схемах (ИС) МСОПД с использованием метода *представления данных путем произвольного доступа*, с целью увеличения емкости машиносчитываемых данных по усмотрению государства или организации выдачи.

Примечание. Спецификации, приводимые в добавлении 1, применяются только к LDS, поддерживающей биометрическую аутентификацию без использования карточки, т. е. в тех случаях, когда МСОПД предоставляет LDS для машинного подтверждения личности, при котором требуется, чтобы МСОПД был только носителем данных.

A1.2 *Представление файла путем произвольного доступа.* Метод представления файла путем произвольного доступа определен исходя из следующих соображений и предположений:

- Поддерживать широкий спектр реализации. LDS включает множество факультативных элементов данных. Эти элементы включаются для упрощения аутентификации МСОПД, аутентификации законного владельца и ускорения процесса обработки в пунктах проверки документов/лиц.

- Структура данных должна поддерживать:

  – ограниченный или обширный набор элементов данных;
  – многократное повторение конкретных элементов данных;
  – постоянную эволюцию конкретных видов реализации.

- Поддерживать по крайней мере один набор данных прикладной программы.

- Допускать использование других национальных специализированных приложений.

- Поддерживать факультативный метод активной аутентификации документа путем использования хранимой ассиметричной пары ключей. Подробная информация об активной аутентификации приводится в разделе IV "*PKI*".

- Поддерживать быстрый доступ к отдельным элементам данных для ускорения процесса оформления владельца документа:

  – непосредственный доступ к необходимым элементам данных;
  – прямой доступ к шаблонам данных, в частности, к биометрическим данным.

A1.2.1 В целях обеспечения интероперабельности в добавлении 1 определяются:

- протокол инициализации, предотвращения коллизий и передачи данных;

- набор команд;
- использование команд, включая ссылки на защиту;
- структура файла для применения LDS МСОПД ИКАО;
- набор знаков.[7]

A1.3 *Требования к защите.* Для надежного обмена данными необходимо обеспечивать целостность и аутентичность данных. Подробные спецификации содержатся в разделе IV "*PKI*".

A1.4 *Совместимость с существующими международными стандартами.* Совместимость с существующими стандартами имеет важнейшее значение для содействия реализации и обеспечения интероперабельности. Поэтому настоящие спецификации обеспечивают максимальную совместимость со стандартами, упомянутыми в разделе I.

A1.5 *Физические характеристики.* Физические характеристики документа СООТВЕТСТВУЮТ физическим характеристикам, указанным в томе 1.

A1.6 *Местоположение и размеры зон соединения*

A1.6.1 Размер зоны соединения СООТВЕТСТВУЕТ стандарту ИСО/МЭК 14443.

A1.6.2 Местоположение зоны соединения СООТВЕТСТВУЕТ стандарту ИСО/МЭК 14443 для документов размера ПД-1 и устанавливается по усмотрению органа выдачи для документов размера ПД-2.

A1.7 *Электронные сигналы.* Мощность радиочастотного сигнала и интерфейс сигналов СООТВЕТСТВУЮТ стандарту ИСО/МЭК 14443.

A1.8 *Протоколы передачи и ответ на запрос*

A1.8.1 *Протокол передачи.* МСОПД ПОДДЕРЖИВАЕТ протокол полудуплексной передачи, определенный в стандарте ИСО/МЭК 14443-4. МСОПД ПОДДЕРЖИВАЕТ протокол передачи либо типа A, либо типа B.

A1.8.2 *Запрос команды.* Бесконтактная ИС ОТВЕЧАЕТ на запрос команды типа A (REQA) или запрос команды типа B (REQB), давая ответ на запрос типа A (ATQA) или ответ на запрос типа B (ATQB) в зависимости от конкретных обстоятельств.

7. Используется стандарт кодирования UTF-8. Большинство элементов данных, используемых в LDS, представляют собой основные знаки латинского алфавита (ASCII) или двоичные знаки. Такие элементы данных, как "имя, написанное буквами национального алфавита", "место рождения" и т. д., не всегда могут кодироваться с помощью кодового набора для знаков латинского алфавита. Поэтому знаки кодируются с использованием стандарта Unicode: UTF-8. Это кодирование с переменной длиной, сохраняющее транспарентность стандарта ASCII. UTF-8 полностью согласуется со стандартом Unicode и ИСО/МЭК 10646. UTF-8 использует 1 байт для кодирования стандартных знаков ASCII (кодовое значение 0…127). Многие знаки неидеографического письма представляются 2 байтами. Остальные знаки представляются 3 или 4 байтами. Использование UTF-8 обеспечивает простое включение знаков, не соответствующих ASCII, без непроизводительных издержек 2, 3 или 4-байтового представления всех знаков.

A1.8.3 *Выбор прикладной программы.* Электронные МСОПД ПОДДЕРЖИВАЮТ по крайней мере одну прикладную программу следующим образом:

- Одна прикладная программа СОСТОИТ из данных, записанных государством или организацией выдачи [группы данных 1–16], и объекта защиты (EF.SOD), необходимых для подтверждения целостности данных, созданных органом выдачи, и хранящихся в DF1. Объект защиты (EF.SOD) состоит из используемых хэш-групп данных. Подробная информация приводится в разделе IV "*PKI*".

- Вторая прикладная программа, которая не поддерживается в настоящем издании части 3 документа Doc 9303, будет состоять из данных, включаемых принимающими государствами или утвержденными принимающими организациями [группы данных 17–19].

Кроме того, государства или организации выдачи могут пожелать добавить другие прикладные программы. Структура файла вмещает дополнительные прикладные программы, однако описание характеристик таких прикладных программ выходит за рамки этого нормативного добавления.

Прикладные программы МСОПД ВЫБИРАЮТСЯ путем идентификации прикладной программы (AID) в качестве зарезервированного наименования DF. AID СОСТОИТ из зарегистрированного идентификатора прикладной программы (RID), присвоенного ИСО в соответствии со стандартом ИСО/МЭК 7816-5, и собственного добавления к идентификатору прикладной программы (PIX), указанного в настоящем документе.

RID = ‘A0 00 00 02 47’.

Прикладная программа хранящихся данных выдающего органа ИСПОЛЬЗУЕТ PIX = ‘1001’.

A1.8.4 *Защита*

Группы данных 1–16 включительно ЗАЩИЩЕНЫ от записи. Хэш для каждой используемой группы данных ХРАНИТСЯ в объекте защиты (EF.SOD). Объект защиты также СОДЕРЖИТ цифровую подпись используемых хэшей. См. раздел IV "*PKI*".

Только государство или организация выдачи имеют доступ к этим группам данных с правом записи. Таким образом, требования в отношении обмена данными не предъявляются и средства, используемые для достижения защиты от записи, не являются частью этой спецификации.

Группы данных 17, 18 и 19 подлежат определению в версии 2 LDS.

A1.9 *Структура файла*. Информация о МСОПД хранится в файловой системе, определенной в стандарте ИСО/МЭК 7816-4. Файловая система организуется иерархически и содержит выделенные файлы (DF) и элементарные файлы (EF). Выделенные файлы DF содержат элементарные файлы или другие выделенные файлы. Факультативный[8] мастер-файл (MF) может служить основой файловой системы.

DF1 (обязательный), определяемый настоящей спецификацией, содержит выдаваемые элементы данных. Для прикладной программы этот DF имеет название ‘A0 00 00 02 47 10 01’ (зарегистрированный RID и PIX) и отбирается по этому названию. Если ИС имеет MF, он может помещаться в любом месте дерева DF, присоединяемого к MF интегральной схемы.

8. Потребность в мастер-файле обуславливается выбором операционных систем.

В каждой прикладной программе может быть определенное количество "групп данных". Прикладная программа государства или организации выдачи может иметь до 16 групп данных. Группа данных 1 [DG1], составляющая машиносчитываемую зону МСЗ, и группа данных 2, составляющая закодированное изображение лица, являются ОБЯЗАТЕЛЬНЫМИ. Все остальные группы данных являются факультативными. Прикладная программа принимающего государства или утвержденной принимающей организации может иметь три группы данных (DG17–19). Эти три группы являются факультативными. Все группы данных представлены в форме шаблонов данных и имеют индивидуальные теги ASN.1.

A1.9.1 *DF1*

DF1 имеет один файл (называется EF.COM), который содержит общую информацию для прикладной программы. Кратким идентификатором, служащим в качестве файлового идентификатора этого файла, является 30 (‘1E’). Этот файл СОДЕРЖИТ информацию о версии LDS, информацию о версии Unicode и перечень групп данных, имеющихся для прикладной программы. Каждая группа данных ХРАНИТСЯ в одном транспарентном EF. Адресацией файлов EF СЛУЖАТ краткие файловые идентификаторы, указанные в таблице A1-1. EF ИМЕЮТ названия для этих файлов, которые составляются согласно схеме: номер n, EF.DGn, где n – номер группы данных. Названием файла EF, содержащего объект защиты, является EF.SOD. Графически структура файла показана на рис. A1-1.

Таблица A1-1. Обязательная прикладная программа государства или организации выдачи

Группа данных	Название EF	Краткий идентификатор EF	FID	Тег
Общая	EF.COM	‘1E’	‘01 1E’	‘60’
DG1	EF.DG1	‘01’	‘01 01’	‘61’
DG2	EF.DG2	‘02’	‘01 02’	‘75’
DG3	EF.DG3	‘03’	‘01 03’	‘63’
DG4	EF.DG4	‘04’	‘01 04’	‘76’
DG5	EF.DG5	‘05’	‘01 05’	‘65’
DG6	EF.DG6	‘06’	‘01 06’	‘66’
DG7	EF.DG7	‘07’	‘01 07’	‘67’
DG8	EF.DG8	‘08’	‘01 08’	‘68’
DG9	EF.DG9	‘09’	‘01 09’	‘69’
DG10	EF.DG10	‘0A’	‘01 0A’	‘6A’
DG11	EF.DG11	‘0B’	‘01 0B’	‘6B’
DG12	EF.DG12	‘0C’	‘01 0C’	‘6C’
DG13	EF.DG13	‘0D’	‘01 0D’	‘6D’
DG14	EF.DG14	‘0E’	‘01 0E’	‘6E’
DG15	EF.DG15	‘0F’	‘01 0F’	‘6F’
DG16	EF.DG16	‘10’	‘01 10’	‘70’
Объект защиты	$EF.SO_D$	‘1D’	‘01 1D’	‘77’

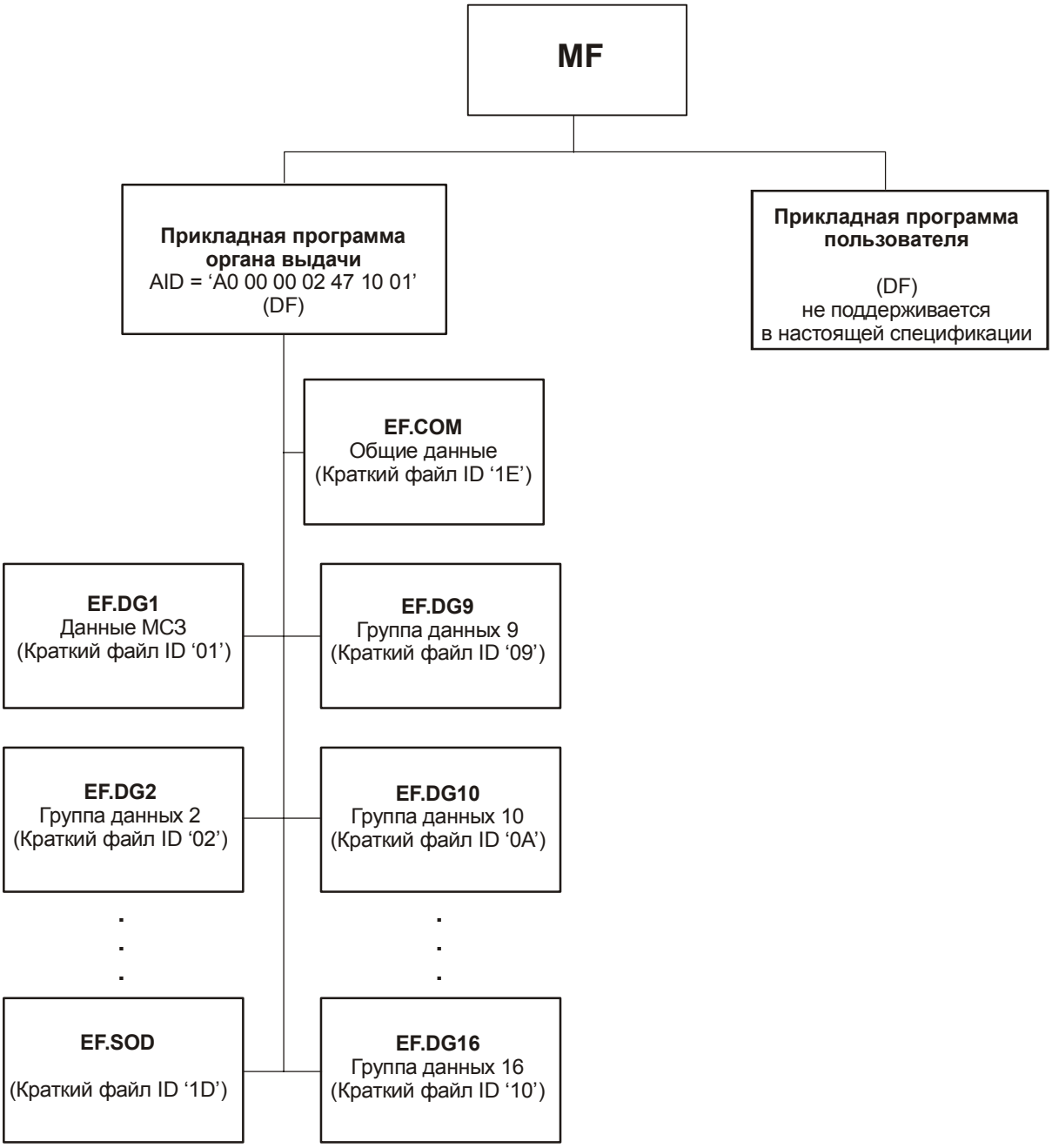

MF
Прикладная программа органа выдачи
AID = ‘A0 00 00 02 47 10 01’
(DF)
Прикладная программа пользователя
(DF)
не поддерживается
в настоящей спецификации
EF.COM
Общие данные
(Краткий файл ID ‘1E’)
EF.DG1
Данные МСЗ
(Краткий файл ID ‘01’)
EF.DG9
Группа данных 9
(Краткий файл ID ‘09’)
EF.DG2
Группа данных 2
(Краткий файл ID ‘02’)
EF.DG10
Группа данных 10
(Краткий файл ID ‘0A’)
EF.SOD
(Краткий файл ID ‘1D’)
EF.DG16
Группа данных 16
(Краткий файл ID ‘10’)

Рис. A1-1.

Каждая группа данных состоит из серии объектов данных, входящих в шаблон. Каждая группа данных ХРАНИТСЯ в отдельном элементарном файле (EF). Индивидуальные объекты данных могут непосредственно извлекаться из группы данных после установления относительной позиции в транспарентном файле.

Файлы содержат элементы данных в качестве объектов данных внутри шаблона. Структура и кодирование объектов данных определяются стандартами ИСО/МЭК 7816-4 и 7816-6. Каждый объект данных имеет идентификационный тег, который устанавливается по шестнадцатеричной системе кодирования (например, ‘5A’). Теги, определяемые в настоящем добавлении, используют вариант кодирования в смешанной структуре. Каждый объект данных имеет индивидуальный тег, длину и значение. Объекты данных, которые могут присутствовать в файле, идентифицируются как обязательные (M) или факультативные (O). Определения содержат конкретную ссылку на номер элемента данных, определяемый в пункте 13. По мере возможности используются межотраслевые теги. Следует отметить, что конкретное определение и формат некоторых тегов изменены для приведения их в соответствие с прикладной программой МСОПД. Например:

Тег 5A определяется как номер документа, а не как номер основного счета, и имеет формат F9N, а не V19N.

Тег 5F20 (имя владельца карточки) переопределен как "Имя владельца" длиной до 39 знаков, кодируемых согласно формату, указанному в Doc 9303.

Тег 65 определяется как отображение фотографии, а не как данные, относящиеся к владельцу карточки.

По мере необходимости дополнительные теги определяются в диапазоне 5F01–5F7F.

A1.10 *Набор команд.* Минимальным набором команд, поддерживаемым МСОПД, ЯВЛЯЕТСЯ следующий набор:

– SELECT

МСОПД поддерживает оба метода (выбор файла и краткий EFID). Считыватели поддерживают по меньшей мере один из двух методов. Идентификатор файла и краткий EFID ОБЯЗАТЕЛЬНЫЕ для систем, использующих чипы, но ФАКУЛЬТАТИВНЫЕ для считывателя.

– READ BINARY

"Le" ДОЛЖЕН быть один бит и ДОЛЖЕН кодироваться согласно стандарту ИСО/МЭК 7816-4.

В зависимости от объема хранимых групп данных, МСОПД будет поддерживать READ BINARY с четным или с четным и нечетным битом INS.

Все команды, форматы и коды их возврата определены в стандарте ИСО/МЭК 7816-4. См. п. A1.20 настоящего добавления, в котором приведены примеры использования этих команд.

Признается, что для надежной загрузки и обновления данных, создания надлежащих условий безопасности и выполнения факультативных положений по защите, указанных в разделе IV "*PKI*", требуются дополнительные команды. Такие команды могут включать:

– GET CHALLENGE;

– EXTERNAL AUTHENTICATE;
– MSE;
– CDS;
– VERIFY CERTIFICATE.

A1.11 *Данные прикладной программы выдающего органа*

Данные прикладной программы выдающего органа, AID = ‘A0 00 00 02 47 10 01’. Прикладная программа выдающего органа состоит из двух обязательных групп данных и четырнадцати факультативных групп данных. Информация, общая для всех групп данных, хранится в прикладном шаблоне ‘60’. Этот шаблон хранится в обязательном файле EF.COM.

A1.11.1 *EF.COM. Общие элементы данных (краткий файл ID = 30 (‘1E’))*

Тег прикладного шаблона ‘60’ – информация об уровне прикладной программы.

Примечание. Этот шаблон в настоящее время содержит только информацию об уровнях пересмотренных версий и список тегов ‘5C’. Структура шаблона определена для поддержки будущих разработок, таких, как динамические подписи и шаблоны биометрической информации (BIT).

В этом шаблоне могут иметь место нижеуказанные элементы данных:

Тег	**Дл.**	**Значение**
‘5F01’	04	Номер версии LDS в формате aabb, где aa обозначает версию LDS, a bb – уровень модификации
‘5F36’	06	Номер версии Unicode в формате aabbcc, где aa обозначает основную версию, bb – вспомогательную версию, a cc – уровень версии программного продукта
‘5C’	X	Список тегов. Список всех имеющихся групп данных

Ниже приводится пример реализации версии 1.7 LDS с использованием версии 4.0.0 Unicode при наличии групп данных 1 (тег ‘61’), 2 (тег ‘75’), 4 (тег ‘76’) и 12 (тег ‘6C’).

В этом и других примерах теги печатаются **жирным шрифтом**, длина – *курсивом*, а значение – латинским шрифтом. Шестнадцатеричные теги, длина и значения приводятся в (‘xx’).

‘60’ *‘16’*
‘5F01’ *‘04’* ‘0107’
‘5F36’ *‘06’* ‘040000’
‘5C’ *‘04’* ‘6175766C’

В полном шестнадцатеричном представлении данный пример будет читаться следующим образом:

‘60’ *‘16’*
‘5F01’ *‘04’* ‘30313037’
‘5F36’ *‘06’* ‘303430303030’
‘5C’ *‘04’* ‘6175766C’

Гипотетическая версия 15.99 LDS будет кодироваться так:

‘60’ *‘16’*
‘5F01’ *‘04’* ‘1599’
‘5F36’ *‘06’* ‘040000’
‘5C’ *‘04’* ‘6175766C’

или так в шестнадцатеричном представлении:

‘60’ *‘16’*
‘5F01’ *‘04’* ‘31353939’
‘5F36’ *‘06’* ‘303430303030’
‘5C’ *‘04’* ‘6175766C’

A1.11.2 *EF.DG1. Информационный тег машиносчитываемой зоны = ‘61’ – ОБЯЗАТЕЛЬНАЯ ИНФОРМАЦИЯ*

Этот EF содержит обязательную информацию машиносчитываемой зоны (МСЗ) документа в шаблоне ‘61’. Шаблон содержит один объект данных (МСЗ в объекте данных ‘5F1F’). Объект данных МСЗ является составным элементом данных, который идентичен информации МСЗ, напечатанной в документе в формате OCR-B.

Тег	Дл.	Значение
‘5F1F’	F	Объект данных МСЗ как составной элемент данных (ОБЯЗАТЕЛЬНЫЙ). (Этот элемент данных содержит все тринадцать примитивных полей – от типа документа до составной контрольной цифры)

Ниже приводится описание структуры элементов данных МСЗ для МСОПД размеров ПД-1 и ПД-2.

Следует отметить, что теги не используются в рамках этого составного элемента данных. Они включаются только для ссылок. Их можно использовать после разбивки объекта данных на уникальные элементы данных.

Примечание. A – буквенный знак [A…Z], N – цифровой знак [0…9], S – специальный знак [‘<’], F – поле фиксированной длины.

EF.DG1 для МСОПД размера 1 (ПД-1)					
Поле	**Содержание**	**Обязат. (M)/ факульт. (O)**	**Формат**	**Пример**	**Тег (только для информации)**
1	Код документа	M	F (2) A,S	I<	5F03
2	Государство или организация выдачи	M	F (3) A,S	NLD	5F28
3	Номер документа	M	F (9) A,N,S[9]	XI85935F8	5A
4	Контрольная цифра – номер документа	M	F (1) N,S	6 или <	5F04

9. Если длина номера документа превышает 9 знаков, то в следующем поле контрольной цифры (поле 5) ставится знак ‘<‘, а остальные цифры номера документа ставятся в факультативном поле данных, следующим сразу за контрольной цифрой номера документа.

EF.DG1 для МСОПД размера 1 (ПД-1)					
Поле	**Содержание**	**Обязат. (М)/ факульт. (О)**	**Формат**	**Пример**	**Тег (только для информации)**
5	Факультативные данные	M	F (15) A,N,S	999999990<<<<<<	53
6	Дата рождения	M	F (6) N,S	720814 (yymmdd)	5F57
7	Контрольная цифра – дата рождения	M	F (1) N	8	5F05
8	Пол	M	F (1) A,S	F, M, или <	5F35
9	Дата истечения срока действия	M	F (6) N	110826 (yymmdd)	59
10	Контрольная цифра – дата истечения срока действия	M	F (1) N	9	5F06
11	Гражданство	M	F (3) A,S	NLD	5F2C
12	Факультативные данные	M	F (11) A,N,S	<<<<<<<<<<<	53
13	Контрольная цифра – общая	M	F (1) N	4	5F07
14	Имя владельца[10]	M	F (30) A,N,S	VAN<DER<STEEN<< MARIANNE<LOUISE	5B

Ниже приведен пример DG1 с использованием этой информации в МСОПД размера ПД-1. Длина элемента данных МСЗ составляет 90 байтов (‘5A’).

‘61’ *‘5B’* **‘5F1F’** *‘5A’*
I<NLDXI85935F86999999990<<<<<<7208148F1108268NLD<<<<<<<<<<<4VAN<DER<STEEN<<MARIANNE<LOUISE

Примечание. A – буквенный знак [A…Z], N – цифровой знак [0…9], S – специальный знак [‘<’], F – поле фиксированной длины.

EF.DG1 для МСОПД размера 2 (ПД-2)					
Поле	**Содержание**	**Обязат. (М)/ Факульт.(О)**	**Формат**	**Пример**	**Тег (только для информации)**
1	Тип документа	M	F (2) A,S	I<	5F03
2	Государство или организация выдачи	M	F (3) A,S	ATA	5F28
3	Имя владельца[11]	M	F (31) A,N,S	SMITH<<JOHN<T<< <<<<<<<<<<<<<<<	5B
4	Номер документа	M	F (9) A,N,S[12]	123456789	5A

10. Правила сокращения имен, которые не вмещаются в поле имени МСЗ, содержатся в томе 1.

11. Правила сокращения имен, которые не вмещаются в поле имени МСЗ, содержатся в томе 1.

12. Если длина номера документа превышает 9 знаков, то в следующем поле контрольной цифры (поле 5) ставится знак ‘<‘, а остальные цифры номера документа ставятся в факультативном поле данных, следующем сразу за контрольной

EF.DG1 для МСОПД размера 2 (ПД-2)					
Поле	**Содержание**	**Обязат. (М)/ Факульт.(О)**	**Формат**	**Пример**	**Тег (только для информации)**
5	Контрольная цифра – номер документа	M	F (1) N,S	1 или <	5F04
6	Гражданство	M	F (3) A,S	NMD	5F2C
7	Дата рождения	M	F (6) N,S	740622 (yymmdd)	5F57
8	Контрольная цифра – дата рождения	M	F (1) N	2	5F05
9	Пол	M	F (1) A,S	F, M, или <	5F35
10	Дата истечения срока действия или действителен до (дата)	M	F (6) N	101231 (yymmdd)	59
11	Контрольная цифра – дата истечения срока действия	M	F (1) N	3	5F06
12	Факультативные данные	M	F (7) A,N,S	0121<<<	53
13	Контрольная цифра – составная	M	F (1) N	4	5F07

Ниже приведен пример DG1 с использованием этой информации в МСОПД размера ПД-2. Длина элемента данных МСЗ составляет 72 байта (‘48’).

‘61’ *‘5B’* **‘5F1F’** *‘48’*
I<ATASMITH<<JOHN<T<<<<<<<<<<<<<<<<<<<<<<<<<123456789<HMD7406222M10123130121<<<54

A1.11.3 *EF.DG2 – EF.DG4 (Один EF для каждой DG) Теги биометрических шаблонов = ‘’75’ ‘63’ ‘76’*

Группы DG2–DG4 используют вариант стандарта ИСО/МЭК 7816-11, предусматривающий вложение без использования карточки (таблица C-10), для обеспечения возможности хранения нескольких биометрических шаблонов определенного типа, соответствующих общему формату файлов обмена биометрическими данными (CBEFF), NISTR 6529a. Биометрический подзаголовок определяет тип имеющейся биометрической информации и конкретную биометрическую характеристику.

Примечания:

Вариант стандарта ИСО/МЭК 7816-11, предусматривающий вложение (таблица C-10), должен использоваться всегда и даже при кодировании одного биометрического шаблона. Последний случай указывается числовым кодированием n=1.

Для указания CBEFF используется установленный по умолчанию идентификатор OID. Элемент данных ‘06’, указанный в стандарте ИСО/МЭК 7816-11, в эту структуру не включается. Аналогичным образом в структуре не определяется полномочие на распределение тегов.

цифрой номера документа. В приведенном выше примере общая длина номера документа составляет 12 (значение = 123456789012), а контрольная цифра = 1.

В целях обеспечения интероперабельности первой биометрической информацией, записываемой в каждой группе данных, ЯВЛЯЕТСЯ интероперабельный на международном уровне блок биометрических данных (ИСО SC37). См. раздел II.

В целях обеспечения конфиденциальности блок биометрических данных может шифроваться с использованием шаблонов безопасного обмена сообщениями, определяемых в добавлении D к стандарту ИСО/МЭК 7816-11. Такая реализация выходит за рамки настоящей спецификации.

Каждый вложенный шаблон имеет следующую структуру.

Тег	**Дл.**	**Значение**				
‘7F61’	**X**	**Шаблон группы биометрической информации**				
		Тег	**Дл.**	**Значение**		
		‘02’	1	Целое число – количество примеров этого типа биометрического параметра		
		‘7F60’	X	Первый шаблон биометрической информации		
			Тег	**Дл.**		
			‘A1’	X	Шаблон заголовка биометрической информации (BHT)	
				Тег	**Дл.**	**Значение**
				‘80’	‘02’	Версия ‘0101’ заголовка ИКАО (факультативная информация) – версия основного формата заголовка CBEFF
				‘81’	‘01-03’	Биометрический тип (факультативная информация)
				‘82’	‘01’	Биометрический подтип (факультативная информация для DG2, обязательная для DG3, DG4)
				‘83’	‘07’	Дата и время создания (факультативная информация)
				‘85’	‘08’	Срок действия (с … по) (факультативная информация)
				‘86’	‘02’	Создатель контрольных биометрических данных (PID) (факультативная информация)
				‘87’	‘02’	Владелец формата (обязательная информация)
				‘88’	‘02’	Тип формата (обязательная информация)
			‘5F2E’ или ‘7F2E’	x	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	
		Тег	**Дл.**			
		‘7F60’	X	Второй шаблон биометрической информации		
			Тег	**Дл.**		
			‘A1’	X	Шаблон заголовка биометрической информации (BHT)	
				Тег	**Дл.**	**Значение**
				‘80’	‘02’	Версия ‘0101’ заголовка ИКАО (факультативная информация) – версия основного формата заголовка CBEFF
				‘81’	‘01’	Биометрический тип (факультативная информация)
				‘82’	‘01’	Биометрический подтип (факультативная информация для DG2, обязательная для DG3, DG4)
				‘83’	‘07’	Дата и время создания (факультативная информация)
				‘85’	‘08’	Срок действия (с … по) (факультативная информация)
				‘86’	‘04’	Создатель контрольных биометрических данных (PID) (факультативная информация)
				‘87’	‘02’	Владелец формата (обязательная информация)
				‘88’	‘02’	Тип формата (обязательная информация)
			‘5F2E’ или ‘7F2E’	x	Биометрические данные (закодированные по правилам владельца формата), именуемые также блоком биометрических данных (BDB)	

Каждый отдельный шаблон биометрической информации имеет нижеуказанную структуру. Заданные теги шаблонов заголовков биометрической информации и их заданные значения являются тем минимумом, который должен поддерживаться каждой реализацией.

Пример:

Один подписанный биометрический параметр лица с длиной блока биометрических данных 12 642 байта (‘3162’ байта), закодированный с использованием устройства, имеющего PID ‘00 01 00 01’, и типа формата ‘00 04’, принадлежащего провайдеру шаблона ‘00 0A’, был взят 15 марта 2002 года (без смещения относительно времени UTC) и действителен с 1 апреля 2002 года по 31 марта 2007 года. Используется основная версия 1.0 шаблона ИКАО.

Общая длина шаблона 12 704 байта. Шаблон записывается в начале EF.DG2 (SFID 02).

‘75’ *‘82319EC’*
- **‘7F61’** *‘823199’*
  - **‘02’** *‘01’* ‘01’
  - **‘7F60’** *‘823191’*
  - **‘A1’** *‘26’*
    - **‘80’** *‘02’* ‘0101’
    - **‘81’** *‘01’* ‘02’
    - **‘83’** *‘07’* ‘20020315133000’
    - **‘85’** *‘08’* ‘20020401200703 31’
    - **‘86’** *‘04’* ‘00010001’
    - **‘87’** *‘02’* ‘000A’
    - **‘88’** *‘02’* ‘0004’
  - **‘5F2E’** *‘823162’* ‘… 12642 байтов биометрических данных …’

A1.11.4 *EF.DG5 – EF.DG7 (один EF для каждой DG). Шаблон отображаемого изображения*
Тег = ‘65’ отображаемые фотографии Тег = ‘67’ отображаемая подпись или обычная отметка

Тег	**Дл.**	**Значение**
‘02’	1	Целое число – количество примеров этого типа отображаемого изображения (обязательная информация в первом шаблоне. Не используется в последующих шаблонах)
‘5F40’ или ‘5F43’	X	Отображаемая фотография Отображаемая подпись или отметка

Пример. Шаблон изображения с длиной данных отображаемого изображения 2 000 байтов. Длина шаблона составляет 2 008 байтов (‘07D8’).

‘65’ *‘8207D8’*
- **‘02’** *‘01’* 1
- **‘5F40’** *‘8207D0’* ‘….2000 байтов данных изображения …’

Для конкретного типа отображаемого изображения распознаются следующие владельцы форматов:

Отображаемое изображение	Владелец формата
Отображаемое изображение лица	ИСО/МЭК 10918, вариант JFIF
Отображаемый отпечаток пальца	ANSI/NIST-ITL 1-2000
Отображаемая подпись/обычная отметка	ИСО/МЭК 10918, вариант JFIF

A1.11.5 *EF.DG8–EF.DG10. Элементы защиты с помощью машины, теги '68' '69' '6A'*

Эти три группы данных еще предстоит определить. Пока они предоставляются для временного собственного использования. Эти элементы данных могут использовать структуру, аналогичную структуре биометрических шаблонов.

Тег	**Дл.**	**Значение**
'02'	1	Целое число – количество примеров этого типа шаблона (обязательная информация в первом шаблоне. Не используется в последующих шаблонах)
	x	Шаблон заголовка. Детали надлежит определить

A1.11.6 *EF. DG11. Дополнительные персональные данные, тег = 6B*

Эта группа данных используется для представления дополнительных данных о владельце документа. Поскольку все элементы данных, входящие в эту группу, являются факультативными, для определения присутствующих элементов используется список тегов.

Примечание. Этот шаблон может содержать знаки нелатинского шрифта.

Тег	**Дл.**	**Значение**
'5C'	X	Список тегов с перечнем элементов данных в шаблоне
'5F0E'	X	Полное имя владельца документа буквами национального алфавита. Кодируется по правилам Doc 9303
'A0'	'X'	Объект данных об именах, строящийся в зависимости от содержания
'02'	01	Количество других имен
'5F0F'	X	Другое имя, форматированное согласно Doc 9303. Объект данных повторяется столько раз, сколько указано в элементе данных '02'
'5F10'	X	Личный номер
'5F2B'	04	Полная дата рождения yyyymmdd (закодированные данные BCD)
'5F11'	X	Место рождения. Поля отделяются знаком '<'
'5F42'	X	Постоянный адрес. Поля отделяются знаком '<'
'5F12'	X	Телефон
'5F13'	X	Профессия
'5F14'	X	Должность
'5F15'	X	Личное резюме
'5F16'	X	Доказательство гражданства. Сжатое изображение согласно ИСО/МЭК 10918
'5F17'	X	Номера других действительных ПД. Отделяются '<'
'5F18'	X	Информация о задержании

В приведенном ниже примере показаны следующие персональные данные: полное имя (John J. Smith), место рождения (Anytown, MN), постоянный адрес (123 Maple Rd, Anytown, MN), номер телефона 1-612-555-1212 и профессия (Travel Agent). Длина шаблона 99 байтов (*'63'*).

'6B' *'63'*

'5C' *'0A'* **'5F0E' '5F11' '5F42' '5F12' '5F13'**
'5F0E' *'0D'* SMITH<<JOHN<J
'5F11' *'0A'* ANYTOWN<MN
'5F42' *'17'* 123 MAPLE RD<ANYTOWN<MN
'5F12' *'0E'* 1-612-555-1212
'5F13' *'0C'* TRAVEL<AGENT

A1.11.7 *EF.DG12. Дополнительные данные о документе, тег = 6C*

Это группа данных используется для представления дополнительной информации о документе. Все элементы данных в этой группе являются факультативными.

Тег	**Дл.**	**Значение**
'5C'	X	Список тегов с перечнем элементов данных в шаблоне
'5F19'	X	Орган выдачи
'5F26'	'04'	Дата выдачи. yyyymmdd (кодирование BCD)
'A0'	X	Объект данных о других людях, строящийся в зависимости от содержания
'02'	'01'	Количество других людей
'5F1A'	X	Имя другого лица, форматированное по правилам Doc 9303
'5F1B'	X	Подтвердительные записи, замечания
'5F1C'	X	Налоговые/выездные требования
'5F1D'	X	Изображение лицевой стороны документа. Изображение согласно ИСО/МЭК 10918
'5F1E'	X	Изображение оборотной стороны документа. Изображение согласно ИСО/МЭК 10918
'5F55'	'07'	Дата и время персонализации документа yyyymmddhhmmss
'5F56'	X	Серийный номер системы персонализации

В приведенном ниже примере указывается государство выдачи (Соединенные Штаты Америки), дата выдачи (31 мая 2002 года) и одно другое лицо, включенное в документ (Brenda P Smith). Длина шаблона составляет 64 байта ('40').

'6C' *'40'*

'5C' *'06'* **'5F19' '5F26' '5F1A'**
'5F19' *'18'* UNITED STATES OF AMERICA
'5F26' *'08'* 20020531
'5F1A' *'0F'* SMITH<<BRENDA<P

A1.11.8 *EF.DG13. Факультативные данные*

Эта группа данных зарезервирована для конкретных национальных данных. Ее формат определяет страна.

A1.11.9 *EF.DG14. Варианты защиты для вторичных биометрических параметров тег = ‘6E’*

Эта группа данных содержит варианты защиты для вторичных биометрических параметров.

Тег	**Дл.**	**Значение**
‘6E’	X	*зарезервировано — не указано*

A1.11.10 *EF.DG15. Информация об открытом ключе активной аутентификации, тег = ‘6F’*

Эта группа данных содержит информацию об открытом ключе активной аутентификации.

Тег	**Дл.**	**Значение**
‘6F’	X	См. раздел IV "*PKI"*

A1.11.11 *EF.DG16. Уведомляемое лицо(а), тег ‘70’*

В этой группе данных указывается информация, связанная со срочным уведомлением. Она кодируется как серия шаблонов с использованием тег-обозначения ‘Ax’.

Тег	**Дл.**	**Значение**
‘02’	01	Количество шаблонов (указывается только в первом шаблоне)
‘Ax’	X	Начало шаблона, где x (x=1,2,3…) возрастает с каждым экземпляром
‘5F50’	‘04’	Записанная дата
‘5F51’	X	Имя лица
‘5F52’	X	Телефон
‘5F53’	X	Адрес

Пример с двумя записями: Charles R Smith of Anytown, MN и Mary J Brown of Ocean Breeze, CA. Длина шаблона составляет 162 байта (‘A2’).

‘70’ *‘81A2’*

‘02’ *‘01’* 2
‘A1’ ‘4C’
‘5F50’ *‘08’* 20020101
‘5F51’ *‘10’* SMITH<<CHARLES<R
‘5F52’ *‘0B’* 19525551212
‘5F53’ *‘1D’* 123 MAPLE RD<ANYTOWN<MN<55100
‘A2’ ‘4F’

‘5F50’ *‘08’* 20020315
‘5F51’ *‘0D’* BROWN<<MARY<J
‘5F52’ *‘0B’* 14155551212
‘5F53’ *‘23’* 49 REDWOOD LN<OCEAN BREEZE<CA<94000

A1.11.12 *EF.SOD LDS. Объект системы защиты, тег = ‘77’*

Этот EF содержит подписываемую структуру данных согласно RFC3369.

Тег	**Дл.**	**Значение**
‘77’	X	См. раздел IV "PKI"

A1.12 *Прикладная программа принимающего государства*

Не поддерживается структурой LDS в настоящем издании части 3 документа Doc 9303.

A1.13 *Используемые теги*

A1.13.1 Нормативные теги, используемые в LDS

Тег	**Определение**	**Использование**
‘02’	Целое число	Биометрические и отображаемые шаблоны
‘5C’	Список тегов	EF.COM и многие другие
‘5F01’	Номер версии LDS	EF.COM
‘5F08’	Дата рождения (сокращенная)	МСЗ
‘5F09’	Сжатое изображение (ANSI/NIST-ITL 1-2000)	Отображаемый отпечаток пальца
‘5F0A’	Элементы защиты. Закодированные данные	Элементы защиты (детализация TBD)
‘5F0B’	Элементы защиты. Структура	Элементы защиты (детализация TBD)
‘5F0C’	Элементы защиты	Элементы защиты (детализация TBD)
‘5F0E’	Полное имя (знаками национального алфавита)	Дополнительные персональные данные
‘5F0F’	Другие имена	Дополнительные персональные данные
‘5F10’	Личный номер	Дополнительные персональные данные
‘5F11’	Место рождения	Дополнительные персональные данные

Тег	Определение	Использование
‘5F12’	Телефон	Дополнительные персональные данные
‘5F13’	Профессия	Дополнительные персональные данные
‘5F14’	Должность	Дополнительные персональные данные
‘5F15’	Персональное резюме	Дополнительные персональные данные
‘5F16’	Доказательство гражданства (изображение 10918)	Дополнительные персональные данные
‘5F17’	Номера других действительных ПД	Дополнительные персональные данные
‘5F18’	Информация о задержании	Дополнительные персональные данные
‘5F19’	Орган выдачи	Дополнительные данные о документе
‘5F1A’	Другие лица в документе	Дополнительные данные о документе
‘5F1B’	Подтвердительные надписи/замечания	Дополнительные данные о документе
‘5F1C’	Налоговые/выездные требования	Дополнительные данные о документе
‘5F1D’	Изображение лицевой стороны документа	Дополнительные данные о документе
‘5F1E’	Изображение оборотной стороны документа	Дополнительные данные о документе
‘5F1F’	Элементы данных МСЗ	Объекты данных МСЗ
‘5F26’	Дата выдачи	Дополнительные данные о документе
‘5F2B’	Дата рождения (8 цифр)	Дополнительные персональные данные
‘5F2E’	Блок биометрических данных	Биометрические данные
‘5F36’	Уровень версии Unicode	EF.COM
‘5F40’	Шаблон сжатого изображения	Отображаемая фотография
‘5F42’	Адрес	Дополнительные персональные данные
‘5F43’	Шаблон сжатого изображения	Отображаемая подпись или отметка

Тег	Определение	Использование
‘5F50’	Записанные данные о дате	Уведомляемое лицо
‘5F51’	Имя лица	Имя уведомляемого лица
‘5F52’	Телефон	Номер телефона уведомляемого лица
‘5F53’	Адрес	Адрес уведомляемого лица
‘5F55’	Дата и время персонализации документа	Дополнительные данные о документе
‘5F56’	Серийный номер системы персонализации	Дополнительные данные о документе
‘60’	Общие элементы данных	EF.COM
‘61’	Шаблон для группы данных МСЗ	
‘63’	Шаблон для группы биометрических данных (о пальце)	
‘65’	Шаблон для цифрового изображения лица	
‘67’	Шаблон для цифровой подписи или обычной отметки	
‘68’	Шаблон для машинной защиты. Закодированные данные	
‘69’	Шаблон для машинной защиты. Структурный	
‘6A’	Шаблон для машинной защиты. Вещественный	
‘6B’	Шаблон для дополнительных персональных данных	
‘6C’	Шаблон для дополнительных данных о документе	
‘6D’	Факультативные данные	
‘6E’	Зарезервировано для будущего использования	
‘70’	Уведомляемое лицо	
‘75’	Шаблон для группы биометрических данных (о лице)	
‘76’	Шаблон для биометрического шаблона (о радужной оболочке глаза)	
‘77’	EF.SOD (EF защиты)	
‘7F2E’	Блок биометрических данных (зашифрованный)	
‘7F60’	Шаблон биометрической информации	
‘7F61’	Шаблон группы биометрической информации	
‘8x’	Теги, зависящие от контекста	CBEFF
‘90’	Зашифрованный хэш-код	Код аутентичности/целостности

Тег	Определение	Использование
‘A0’	Объекты данных, строящиеся в зависимости от контекста	Дополнительные персональные данные
		Дополнительные данные о документе
‘Ax’ или ‘Bx’	Повторяющийся шаблон, где x обозначает экземпляр	Заголовок биометрической информации

A1.13.2 Теги, используемые для промежуточной обработки (информативные)

Тег	Определение	Использование
‘53’	Факультативные данные	Часть MC3
‘59’	Дата истечения срока действия	Часть MC3
‘5A’	Номер документа	Часть MC3
‘5F02’	Контрольная цифра – факультативные данные (только ID-3)	Часть MC3
‘5F03’	Тип документа	Часть MC3
‘5F04’	Контрольная цифра – номер документа	Часть MC3
‘5F05’	Контрольная цифра – дата рождения	Часть MC3
‘5F06’	Контрольная цифра – дата истечения срока действия	Часть MC3
‘5F07’	Контрольная цифра – составная	Часть MC3
‘5B’	Имя владельца документа	Часть MC3
‘5F28’	Государство или организация выдачи	Часть MC3
‘5F2B’	Дата рождения	Часть MC3
‘5F2C’	Гражданство	Часть MC3
‘5F35’	Пол	Часть MC3
‘5F57’	Дата рождения (6 цифр)	Часть MC3

A1.13.3 Теги, зарезервированные для будущего использования (нормативные)

Тег	Определение	Использование
‘5F44’	Страна въезда/выезда	Записи о поездках
‘5F45’	Дата въезда/выезда	Записи о поездках
‘5F46’	Порт въезда/выезда	Записи о поездках
‘5F47’	Указатель въезда/выезда	Записи о поездках

Тег	Определение	Использование
‘5F48’	Продолжительность пребывания	Записи о поездках
‘5F49’	Категория (классификация)	Записи о поездках
‘5F4A’	Ссылка на инспектора	Записи о поездках
‘5F4B’	Указатель въезда/выезда	Записи о поездках
‘71’	Шаблон для электронных виз	
‘72’	Шаблон для схем пересечения границы	
‘73’	Шаблон для групп данных с записями о поездках	

A1.14 *Минимальные требования к обеспечению интероперабельности.* Ниже УКАЗЫВАЮТСЯ минимальные требования к обеспечению интероперабельности МСОПД на бесконтактной ИС с индуктивной связью через малый зазор (см. ИСО/МЭК 14443):

- ИСО/МЭК 14443, части 1–4, и ИСО/МЭК 10373-6 с учетом поправок к обеим сериям стандартов;
- интерфейс сигналов типа A или типа B[13];
- поддержка файловой структуры, определяемой стандартом ИСО/МЭК 7816-4 для записи различной длины;
- поддержка одной или нескольких прикладных программ и соответствующих команд, определяемых стандартом ИСО/МЭК 7816-4, 5.

A1.15 *Команды и параметры команд, которые могут использоваться устройством интерфейса*

A1.15.1 Ниже приводится типичная последовательность обработки для выбора прикладной программы DF1 и извлечения данных из элементарного файла. Аналогичный процесс извлечения (считывания) используется для всех элементарных файлов в DF. Действительность групп данных из DF1 ДОЛЖНА затем верифицироваться путем исчисления хэш-значения группы данных и сравнения его с хэш -значением, полученным из данных системы безопасности EF.SO_D.

Типичная последовательность операций следующая:

- Документ вводится в поле действия устройства соединения через малый зазор (PCD).
- IC отвечает на запрос команды типа A (REQA) или запрос команды типа B (REQB), давая ответ на запрос типа A (ATQA) или ответ на запрос типа B (ATQB) в зависимости от конкретного случая.
- PCD обнаруживает и устраняет любую коллизию, которая может иметь место при нахождении нескольких документов в поле действия.

13. Это означает, что считыватели (устройства соединения через малый зазор) ДОЛЖНЫ быть способны считывать тип A и тип B.

- Выполнение команд, соответствующих стандарту ИСО/МЭК 7816, ОПРЕДЕЛЯЕТСЯ

  – типом A: SAK (Select Acknowledge) бит 6 = 1, бит 3 = 0;
  – типом B: Protocol_Type ="0001".

- Выбирается прикладная программа государства выдачи МСОПД ИКАО.

- Затем элементарные файлы выбираются и считываются по мере необходимости. Аналогичный процесс отбора и считывания используется для всех EF. Форматы команд описываются в конце добавления.

  – EF может выбираться путем указания SFID файла EF в первой команде READ BINARY (первоначальная зона данных). Остальные данные затем считываются с помощью серии основных команд READ BINARY, при этом каждая команда указывает следующую зону данных, подлежащую считыванию.

  – При желании EF может выбираться путем использования команды SELECT. Данные считываются с EF с помощью серии основных команд READ BINARY, при этом каждая команда указывает следующую зону данных, подлежащую считыванию.

Примечание. Поддержка SFI ОБЯЗАТЕЛЬНА для МСОПД. РЕКОМЕНДУЕТСЯ, чтобы проверочные системы использовали SFI

- Сначала считывается общий файл данных EF.COM (краткий идентификатор файла = '1E'), содержащий идентификатор прикладной программы, уровни версии и список тегов в шаблоне '60'.

- В списке тегов в EF.COM перечисляются группы данных (элементарные файлы), присутствующие в DF1. Устройство интерфейса определяет, какая группа данных (EF) должна считываться и использоваться. Затем в каждом EF производится поиск для получения группы данных из EF.

- Машиносчитываемая зона (МСЗ) обычно является первым считываемым EF.

- Другие EF считываются для получения соответствующих групп данных по мере необходимости.

- Затем $EF.SO_D$ считывается для подтверждения целостности групп данных, считанных с DF1.

  Примечание. $EF.SO_D$ МОЖЕТ считываться первым.

A1.16 *Детали инициализации и предотвращения коллизий в соответствии со стандартом ИСО/МЭК 14443, тип A.*

Примечание. Электронный МСОПД может служить “маяком”, в котором бесконтактная ИС излучает номер индивидуального идентификатора (UID). Это позволяет идентифицировать орган выдачи. Согласно стандарту ИСО/МЭК 14443 разрешается выбирать или вариант, когда электронный МСОПД представляет фиксированный идентификатор, назначаемый индивидуально только данному электронному МСОПД, или произвольный номер, который является разным в начале каждого диалога.

Выбор того или иного варианта не ведет к ухудшению интероперабельности, так как считыватель, если он соответствует стандарту ИСО/МЭК 14443, должен понимать оба

метода. РЕКОМЕНДУЕТСЯ использовать произвольный UID, однако государства МОГУТ выбрать вариант применения уникального UID.

Примечание. Бесконтактная ИС называется в стандарте ИСО/МЭК 14443 "Карточка на интегральной схеме с индуктивной связью через малый зазор" (PICC), а проверяющий считыватель называется "Устройство соединения через малый зазор" (PCD). В настоящем дополнении используются сокращения "PICC" и "PCD" в целях единообразия и ясности.

A1.16.1 *REQA и WUPA (запуск типа A).* Карточка на интегральной схеме с индуктивной связью через малый зазор (PICC) после приведения в действие должна находиться в режиме ОЖИДАНИЯ. Она ждет команды и должна опознавать команды REQA И WUPA. Оба сигнала передаются коротким кадром (7 бит).

Команда	b7	b6	b5	b4	b3	b2	b1
REQA = ‘26’	0	1	0	0	1	1	0
WUPA = ‘52’	1	0	1	0	0	1	0

Совместимая PICC ДОЛЖНА отвечать на эти команды; все другие значения в данном контексте не допускаются.

A1.16.2 *ATQA*. После передачи устройством PCD команды REQA все PICC, находящиеся в состоянии ОЖИДАНИЯ, синхронно ДАЮТ ответ ATQA.

После передачи устройством PCD команды WUPA все PICC, находящиеся в состоянии ОЖИДАНИЯ или ПРИОСТАНОВКИ, синхронно ДАЮТ ответ ATQA.

Ответ ATQA состоит из 2 байтов. В соответствии со стандартом ИСО/МЭК 14443-3 MSB содержит только RFU и частные биты пользователя, поэтому эти байты должны игнорироваться любым соответствующим программным обеспечением.

Биты 7 и 8 LSB определяют размер PICC UID согласно следующей таблице:

b8	b7	Значение
0	0	Размер UID: одинарный
0	1	Размер UID: двойной
1	0	Размер UID: тройной
1	1	RFU

Совместимая PICC должна подтверждать один из трех действительных размеров UID.

Биты 1–5 LSB указывают биткадровую антиколлизию. Один и только один из этих битов ДОЛЖЕН быть установлен. Бит 6 является RFU и НЕ ДОЛЖЕН оцениваться никаким программным обеспечением.

A1.16.3 *Антиколлизия и выбор.* В соответствии с размером UID, определяемым ответом ATQA, команда выбора ПОСЫЛАЕТСЯ для каждого каскадного уровня. Если имеет место коллизия, ВАПОЛНЯЕТСЯ антиколлизионный цикл.

A1.16.3.1 Для команды выбора допускаются только значения ‘93’ (каскадный уровень 1), ‘95’ (каскадный уровень 2) и ‘97’ (каскадный уровень 3).

A1.16.3.2 После выполнения антиколлизионного цикла выбирается одна PICC и производится возврат ответа SAK. SAK состоит из одного байта, где только два бита являются значимыми. Бит 3 указывает, что UID еще не полностью передан, а это означает, что должен быть выполнен еще один выборный/антиколлизионный цикл на следующем каскадном уровне.

A1.16.3.3 Если бит 3 не установлен, бит 6 определяет, соответствует ли PICC стандарту ИСО/МЭК 14443-4. Поскольку ТРЕБУЕТСЯ, чтобы все PICC, используемые для хранения данных LDS, поддерживали 14443-4, этот бит должен быть установлен.

A1.16.4 *Запрос ответа на выбор (RATS).* После выполнения антиколлизионного и выборного цикла на PICC ПОСЫЛАЕТСЯ RATS. RATS состоит из фиксированного начального байта ‘E0’ и параметрического байта, который указывает максимальный размер кадра PCD и идентификатора карточки (CID). CID указывается в наименее значимом полубайте; он используется для идентификации PICC, когда она находится в активном состоянии.

Наиболее значимый полубайт (FDSI) содержит максимальный размер кадра (FSD) в соответствии со следующей схемой конверсии.

FDSI	‘0’	‘1’	‘2’	‘3’	‘4’	‘5’	‘6’	‘7’	‘8’	‘9’ — ‘F’
FSD	16	24	32	40	48	64	96	128	256	RFU (>256)

Для передачи данных LDS соответствующее считывающее устройство ДОЛЖНО поддерживать размер кадра в 256 байтов; поэтому наиболее значимый полубайт параметрического байта ДОЛЖЕН быть ‘8’.

A1.16.5 *Ответ на выбор.* Ответ на выбор указывает информацию о возможностях PICC. Он содержит до трех интерфейсных байтов. Первый интерфейсный байт TA (1) содержит параметр PICC по скорости передачи данных в битах. Второй байт TB (1) передает информацию для определения времени ожидания кадра и начала защитного временного интервала кадра. Третий интерфейсный байт TC (1) указывает протокольный параметр. Наименее значимый байт ДОЛЖЕН быть 1, если PICC поддерживает адрес узла NAD. Второй байт должен быть 1, если PICC поддерживает CID.

Все остальные биты являются RFU и ДОЛЖНЫ игнорироваться любым соответствующим программным обеспечением.

За интерфейсными байтами следуют исторические байты. Они содержат общую информацию о PICC и НЕ ДОЛЖНЫ оцениваться соответствующим программным обеспечением.

A1.17 *Данные о форматах команд и параметрических вариантах ИСО/МЭК 7816*

A1.17.1 Выбор прикладной программы

Прикладные программы должны выбираться либо по их файловому идентификатору, либо по названию прикладной программы. После выбора прикладной программы можно получить доступ к файлу в данной программе.

Примечание. Названия прикладных программ должны быть уникальными. Поэтому выбор прикладной программы с использованием ее названия может производиться в любом месте где бы это необходимо.

A1.17.2 Выбор мастер-файла

CLA	INS	P1	P2	Lc	Данные	Le
‘00’	‘A4’	‘00’	‘0C’	0	Незаполнено	–

Примечание. РЕКОМЕНДУЕТСЯ НЕ использовать команду SELECT MF.

A1.17.3 Выбор прикладной программы по идентификатору

Прикладная программа выбирается путем использования названия DF. Параметры команды APDU указаны ниже.

CLA	INS	P1	P2	Lc	Данные	Le
‘00’	‘A4’	‘04’	‘0C’	Var.	AID	–

A1.18 *Выбор EF путем использования команды SELECT*

Файлы должны выбираться по их файловому идентификатору. Когда файлы выбираются по FID, необходимо убедиться в том, что прикладная программа, в которой хранятся файлы, предварительно выбрана.

CLA	INS	P1	P2	Lc	Данные	Le
‘00’	‘A4’	‘02’	‘0C’	‘02’	Файл ID	–

A1.19 *Считывание данных с EF*

В целом имеется два способа считывания данных: путем выбора файла и затем считывания данных или путем прямого считывания данных с использованием SFI. Для МСОПД ОБЯЗАТЕЛЬНО обеспечивается поддержка SFI. Поэтому РЕКОМЕНДУЕТСЯ, чтобы проверочные системы использовали SFI.

A1.19.1. Считывание данных выбранного файла (транспарентный файл)

CLA	INS	P1	P2	Lc	Данные	Le
‘00’	‘B0’	Смещение MSB	Смещение LSB	–	–	MaxRet

Определение P1 и P2:

	b7	b6	b5	b4	b3	b2	b1	b0
Смещение MSB	0	X	X	X	X	X	X	X
Смещение LSB	X	X	X	X	X	X	X	X

A1.19.2 Считывание данных с использованием SFI (транспарентный файл)

CLA	INS	P1	P2	Lc	Данные	Le
‘00’	‘B0’	SFI	Смещение LSB	–	–	MaxRet

Определение P1 и P2:

	b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**
SFI	1	0	0	X	X	X	X	X
Смещение LSB	X	X	X	X	X	X	X	X

A1.20 *Примеры использования ИСО/МЭК 7816 с LDS*

A1.20.1 Считывание данных MC3 с использованием выбора файла

Считывание данных группы данных 1 (MC3) может производиться в следующей последовательности:

CLA	**INS**	**P1**	**P2**	**Lc**	**Данные**	**Le**	**Замечания**
‘00’	‘A4’	‘04’	‘0C’	‘07’	‘A0 00 00 02 47 10 01’	–	Выбор приложения органа выдачи
‘00’	‘A4’	‘02’	‘0C’	‘02’	‘01 01’	–	Выбор DG1
‘00’	‘B0’	‘00’	‘00’	–	–	‘00’	Считывание макс. 256 байтов

A1.20.2 Считывание группы данных 2

A1.20.2.1 Считывание данных группы данных 2 (закодированное изображение лица) может производиться в указанной ниже последовательности. Длина шаблона составляет 12 543 байта. Общая область данных составляет 12 547 байтов (т.е. плюс один байт на тег шаблона и три байта на длину поля). Это требует 49 блоков по 256 байтов каждый плюс заключительный блок в 3 байта.

A1.20.2.2 Следующая часть шаблона считывается путем увеличения смещения на 256 байтов (‘01 00’). Общий объем считываемых данных определяется по длине шаблона. Команду READ BINARY рекомендуется выдавать только для остаточного объема данных. Заключительное смещение – ‘31 00’.

CLA	**INS**	**P1**	**P2**	**Lc**	**Данные**	**Le**	**Замечания**
‘00’	‘A4’	‘04’	‘0C’	‘07’	‘A0 00 00 02 47 10 01’	–	Выбор приложения органа выдачи
‘00’	‘A4’	‘02’	‘0C’	‘02’	‘01 02’	–	Выбор DG2
‘00’	‘B0’	‘00’	‘00’	–	–	‘00’	Считывание первых 256 байтов
‘00’	‘B0’	‘01’	‘00’	–	–	‘00’	Считывание следующих 256 байтов
‘00’	‘B0’	‘02’	‘00’	–	–	‘00’	Считывание следующих 256 байтов
‘00’	‘B0’	‘03’	‘00’	–	–	‘00’	:

A1.20.2.3 При последовательном считывании более одной группы данных выбор прикладной программы органа выдачи должен производиться только один раз (перед считыванием первого файла).

A1.20.3 Считывание данных MC3 с использованием глобального SFI

CLA	INS	P1	P2	Lc	Данные	Le	Замечания
‘00’	‘B0’	‘81’	‘00’	–	–	‘00’	Прямое считывание 256 байтов

A1.20.4 Считывание группы данных 2 с использованием глобального SFI

Первые байты файла могут считываться с использованием команды Read Binary в сочетании с SFI. Следующие байты должны считываться с использованием “стандартной” команды Read Binary.

CLA	INS	P1	P2	Lc	Данные	Le	Замечания
‘00’	‘B0’	‘82’	‘00’	–	–	‘00’	Прямое считывание 256 байтов
‘00’	‘B0’	‘01’	‘00’	–	–	‘00’	Считывание следующих 256 байтов
‘00’	‘B0’	‘02’	‘00’	–	–	‘00’	Считывание следующих 256 байтов
‘00’	‘B0’	‘03’	‘00’	–	–	‘00’	:

A1.21 *EF размером более 32 767 байтов*

Максимальный размер EF обычно составляет 32 767 байтов, однако некоторые ИС поддерживают более крупные файлы. При смещении свыше 32 767 для доступа к области данных требуется иной параметрический вариант и формат команды READ BINARY. Этот формат команды следует использовать после установления длины шаблона и потребности в доступе к данным в расширенной области данных. Например, если область данных содержит несколько объектов биометрических данных, считывать всю область данных, возможно, не требуется. При смещении на область данных свыше 32 767 используется этот формат команды. Смещение ставится в поле команд, а не в параметрах P1 и P2.

CLA	INS	P1	P2	Lc	Данные	Le	Замечания
‘00’	‘B1’	‘00’	‘00’	Var.	*Закодированное смещение TLV*	‘00’	Считывание файлов размером более 32 767 байтов

Длина поля и значение поля в объекте данных BER-TLV ДОЛЖНЫ быть как можно более короткими. Это имеет отношение не только к объектам данных о смещении в командах Odd INS READ BINARY, но также и ко всем другим объектам данных BER-TLV, обмен которыми осуществляется между электронным МСОПД и терминалом.

Пример закодированного смещения в поле данных:

Смещение: ‘FF FF’ кодируется как ‘54 02 ff ff’.

Последующие команды READ BINARY указывают смещение в поле данных. Заключительная команда READ BINARY должна запрашивать остальную область данных.

A1.22 *Правила кодирования длины ASN.1 BER*

ДОЛЖНА использоваться *определенная* форма кодирования длины (как указано в п.8.1.3.1 ИСО/МЭК 8825-1 (ASN.1)).

Диапазон	№ байтов	1-й байт	2-й байт	3-й байт
0–127	1	двоичное значение	нет	нет
128–255	2	‘81’	двоичное значение	нет
256–65 535	3	‘82’	двоичное значение MS байт LS байт	
MS – наиболее значимый байт; LS – наименее значимый байт				

Примечание. Знак (‘ ’) используется для визуального разделения шестнадцатеричных знаков. Они не кодируются в LDS.

A1.22.1 Примеры, основанные на сформулированных выше правилах:

Пример 1: длина в тридцать девять (39) кодируется как ‘27’ в шестнадцатеричном представлении.

Пример 2: длина в сто девяносто девять (199) кодируется как ‘81C7’ в шестнадцатеричном представлении.

Пример 3: длина в одну тысячу (1000) кодируется как ‘8203E8’ в шестнадцатеричном представлении.

A1.23 *Кодирование биометрических подхарактеристик*

В таблице A1-2 показана схема кодирования подхарактеристик:

Таблица A1-2. CBEFF

b8	b7	b6	b5	b4	b3	b2	b1	Биометрический подтип
0	0	0	0	0	0	0	0	Информация не дается
						0	1	Правый
						1	0	Левый
			0	0	0			Не имеет значения
			0	0	1			Большой палец
			0	1	0			Указательный
			0	1	1			Средний
			1	0	0			Безымянный
			1	0	1			Мизинец
x	x	x						Зарезервировано для будущего использования

РАЗДЕЛ IV

PKI ДЛЯ МАШИНОСЧИТЫВАЕМЫХ ПРОЕЗДНЫХ ДОКУМЕНТОВ С ДОСТУПОМ К ICC ТОЛЬКО ДЛЯ СЧИТЫВАНИЯ

1. СФЕРА ПРИМЕНЕНИЯ

1.1 В настоящем разделе приводятся спецификации, позволяющие государствам и поставщикам внедрить схему аутентификации, включающую конкретную инфраструктуру применения и использования современных схем инфраструктуры открытых ключей (PKI) для внедрения и использования электронных цифровых подписей для машиносчитываемых проездных документов (МСПД), предоставляющих доступ к ICC только для считывания.

1.2 Данные спецификации не предписывают полного внедрения сложной структуры PKI в каждой стране. Они предназначены скорее для определения способа внедрения, при котором государства могут делать выбор в различных сферах (таких, как активная или пассивная аутентификация, защита от скимминга и контроль доступа или автоматизированное пересечение границ) и иметь таким образом возможность поэтапно вводить дополнительные элементы, не нарушая структурной основы.

2. ДОПУЩЕНИЯ

2.1 Предполагается, что читатель знаком с концепциями и механизмами, предоставляемыми криптографией с открытым ключом и инфраструктурами открытых ключей.

2.2 Хотя использование техники криптографии с открытым ключом усложняет введение электронных МСОПД, включающих интегральную схему, такая техника полезна тем, что она предоставляет в распоряжение пунктов пограничного контроля дополнительное средство установления подлинности МСОПД. Предполагается, что ее использование не является единственной мерой установления аутентичности и НЕ СЛЕДУЕТ полагаться не нее как на единственный определяющий фактор.

2.3 Изображение лица, хранящееся в цифровой форме, как предполагается, не является информацией, затрагивающей личную жизнь. Изображение лица владельца МСОПД также печатается в документе и может быть легко получено.

2.4 Хранящиеся в цифровой форме изображения пальца(ев) и/или радужной оболочки глаза являются дополнительными биометрическими характеристиками, которые МОГУТ выбираться государствами для внутреннего использования. Они, как правило, считаются информацией, затрагивающей личную жизнь, и, следовательно, должны защищаться в соответствии с национальным законодательством государства выдачи.

2.5 Маловероятно, что ИКАО или какая-то другая единственная центральная организация будет устанавливать, поддерживать или контролировать защищенные закрытые ключи для

какого-либо государства. Несмотря на множество стратегических альянсов среди участников, этот вариант не будет признан в качестве решения, заслуживающего доверия.

2.6 В случае невозможности использования данных с бесконтактной ИС, например в результате отзыва сертификата или недействительной верификации подписи, или если бесконтактная ИС была умышленно оставлена пустой (как описывается в п. 7.1 настоящего раздела), МСОПД вовсе не обязательно становится недействительным. В таком случае принимающее государство МОЖЕТ полагаться на другие элементы защиты документа в целях валидации.

2.7 Списки отзыва сертификатов (CRL) используются только для сертификатов подписывающего полномочного органа (CA) страны и сертификатов лиц, подписывающих документы. CRL не применяются к индивидуальным объектам защиты и конкретным парам ключей активной аутентификации документов.

3. ТЕРМИНОЛОГИЯ

3.1 CA, ключи и сертификаты

В рамках настоящего раздела значение имеют следующие ключи и сертификаты:

Название	**Сокращение**	**Замечания**
Подписывающийся CA страны	CSCA	
Сертификат подписывающегося CA страны	C_{CSCA}	Выдается CSCA (самоподписанный). Содержит открытый ключ подписывающегося CA страны (KPu_{CSCA}). Хранится в системе проверки
Закрытый ключ подписывающегося CA страны	KPr_{CSCA}	Подписывание сертификата лица, подписывающего документы (C_{DS}). Хранится в условиях (повышенной) защиты в государстве выдачи
Открытый ключ подписывающегося CA страны	KPu_{CSCA}	Для верификации подлинности сертификата лица, подписывающего документы (C_{DS})
Лицо, подписывающее документы	DS	
Сертификат лица, подписывающего документы	C_{DS}	Выдается подписывающимся CA страны (CSCA). Содержит открытый ключ лица, подписывающего документы (KPu_{DS}). Хранится в системе проверки и/или на бесконтактной ИС МСОПД
Закрытый ключ лица, подписывающего документы	KPr_{DS}	Подписывание объекта защиты документа (SO_D). Хранится в условиях (повышенной) защиты в государстве выдачи
Открытый ключ лица, подписывающего документы	KPu_{DS}	Для верификации подлинности объекта защиты документа (SO_D)
Объект защиты документа	SO_D	Подписанная структура данных RFC3369 CMS, подписываемая лицом, подписывающим документы (DS).

Название	Сокращение	Замечания
		Содержит хэшированные группы данных LDS. Хранится на бесконтактной ИС МСОПД. МОЖЕТ содержать сертификат лица, подписывающего документы (C_{DS})
Закрытый ключ активной аутентификации	KPr_{AA}	ФАКУЛЬТАТИВНЫЙ. Вычисление подписи в механизме активной аутентификации на бесконтактной ИС МСОПД. Хранится в защищенной памяти бесконтактной ИС
Открытый ключ активной аутентификации	KPu_{AA}	ФАКУЛЬТАТИВНЫЙ. Верификация подписи в механизме активной аутентификации на бесконтактной ИС МСОПД
Базовые ключи доступа к документу	K_{ENC} и K_{MAC}	ФАКУЛЬТАТИВНЫЕ. Для получения доступа к открытым данным МСОПД и для защиты передачи сообщений между бесконтактной ИС МСОПД и системой проверки

3.2 Термины, определения и сокращения

Глоссарий терминов, определений и сокращений приведен в начале этого тома.

4. СПРАВОЧНЫЕ МАТЕРИАЛЫ

Некоторые положения упоминаемых в этом тексте международных стандартов стали положениями настоящего тома. Эти справочные материалы перечислены в п. 5 раздела I.

5. ОБЩИЕ ПОЛОЖЕНИЯ

5.1 Принципы схем PKI получили развитие в процессе их использования и стали весьма сложными в применении к современным сценариям. Они используются прежде всего в операциях по Интернету, требующих доверия к ключам со стороны широкого круга пользователей и агентств; в результате появились сложные системы сертификатов ключей, где открытые ключи выдаются в "сертификатах", которые в цифровой форме подписываются доверенными организациями выдачи, именуемыми сертифицирующими полномочными органами (CA). Доверие к этим CA далее подтверждается CA более высокого уровня в иерархической лестнице доверия, причем каждый в этой иерархии выдает ключ и подписывает сертификат в отношении нижестоящего по иерархии подчинения. Высшим уровнем в такой иерархии является так называемый "корневой CA". Различные иерархии перекрестно сертифицируют друг друга с целью создания уверенности в совместно выдаваемых ключах.

5.2 Осложняющим фактором является потребность в списках отзыва сертификатов (CRL), в которых указывается какой ключ (сертификат) утратил силу по какой-либо причине. Фактически актом отзыва сертификата и опубликования информации об отзыве в CRL, орган, выдавший сертификат, информирует принимающие стороны о том, что его содержанию доверять больше нельзя. Необходимость верифицировать сертификаты при каждой и всякой операции часто предполагает многократные обращения к записям CA и записям CRL в различных базах данных. Это является сложным требованием.

5.3 Условия использования МСОПД, отвечающих стандартам ИКАО, отличаются от вышеупомянутых коммерческих условий, где вопрос отзыва открытых ключей решается иным способом (по сравнению с индивидуальными пользователями), поскольку маловероятный случай компрометации закрытого ключа государства, который использовался в течение определенного периода для подписания многих МСОПД, не может быть отрицанием того, что документы действительно подписывались с использованием этого ключа. Этими (действительными) документами их владельцы по-прежнему пользуются для совершения поездок. Применяемые электронные цифровые подписи рассчитаны на весь срок действия МСОПД и не предназначены для целей повседневных операций. В случае компрометации ключа ДОЛЖЕН использоваться механизм предостережения для предупреждения государств о необходимости более тщательного просмотра таких документов.

5.4 В связи с этим в настоящем томе документа Doc 9303 излагается специализированный подход, позволяющий сообществу пользователей МСПД быстро внедрить этот вид применения МСОПД с доступом к ICC только для считывания и воспользоваться его преимуществами, и не предпринимается никаких попыток рассмотреть более крупные вопросы политики PKI и сложные иерархии. Сертификаты используются в целях безопасности наряду с предлагаемой методологией рассылки открытых ключей (сертификатов) государствам-членам, и данная инфраструктура приспособлена к целям ИКАО.

5.5 Обязанности

Применение PKI ИКАО осуществляется на полностью равноправных условиях между пользователями, причем каждое государство является независимым и самостоятельным в вопросах МСОПД и безопасности. Тем не менее неотъемлемой частью программы является наличие эффективного и общепринятого средства совместного использования и обновления в любой момент набора действующих открытых ключей ко всем существующим действительным МСОПД всех участвующих государств.

5.5.1 *Государства выдачи*

Каждое участвующее государство ИМЕЕТ собственные надежные средства создания наборов ключей на различные периоды времени; каждый такой набор ИСПОЛЬЗУЕТСЯ для вычисления электронных цифровых подписей, применяемых для подписания сертификатов. Эти системы или средства надежно ПРЕДОХРАНЯЮТСЯ от любого внешнего или несанкционированного доступа за счет собственной конструкции и средств защиты аппаратуры.

Подписывающийся CA страны

Иерархия CA, в которой генерируются ключи, имеет отношение к настоящему разделу лишь в той мере, в какой она включает сертификаты, направляемые принимающим государствам. Направленный сертификат высшего уровня ЯВЛЯЕТСЯ предметом доверия для принимающего государства. В настоящем разделе такой сертификат именуется сертификатом подписывающегося CA страны (C_{CSCA}). Сертификат подписывающегося CA страны (C_{CSCA}) САМОПОДПИСЫВАЕТСЯ и выдается подписывающимся CA страны (CSCA).

РЕКОМЕНДУЕТСЯ, чтобы пары ключей подписывающегося CA страны (KPu_{CSCA}, KPr_{CSCA}) генерировались и хранились в надежно защищенной автономной инфраструктуре CA государством выдачи.

Сертификаты подписывающегося СА страны (C_{CSCA}) ДОЛЖНЫ распределяться только по надежным дипломатическим каналам (внеполосное распределение).

Каждый сертификат подписывающегося СА страны (C_{CSCA}), создаваемый каждым государством, ДОЛЖЕН также направляться в ИКАО (с целью валидации сертификатов лиц, подписывающих документы (C_{DS})).

Закрытый ключ подписывающегося СА страны (KPr_{CSCA}) используется для подписания сертификатов лиц, подписывающих документы (C_{DS}).

В добавлении 1 указаны профили сертификатов.

Лицо, подписывающее документы

РЕКОМЕНДУЕТСЯ, чтобы пары ключей лица, подписывающего документы (KPu_{DS}, KPr_{DS}), генерировались и хранились в надежно защищенной инфраструктуре СА государством выдачи.

Каждый сертификат лица, подписывающего документы (C_{DS}), генерируемый каждым государством, ДОЛЖЕН направляться в ИКАО и МОЖЕТ храниться на бесконтактной ИС МСОПД.

Закрытый ключ лица, подписывающего документы (KPr_{DS}), используется для подписания объектов защиты документов (SO_D).

Каждый объект защиты документов (SO_D), генерируемый каждым государством, ДОЛЖЕН храниться на соответствующей бесконтактной ИС МСОПД.

В добавлении 1 указаны профили сертификатов.

Отзыв сертификатов

В случае инцидента (например компрометации ключа) государства выдачи могут отзывать сертификаты. Информация о таком отзыве ДОЛЖНА направляться в двустороннем порядке всем другим участвующим государствам и Директории открытых ключей ИКАО в течение 48 ч.

При отсутствии инцидентов государствам выдачи СЛЕДУЕТ направлять "рутинные" CRL друг другу и Директории открытых ключей ИКАО по крайней мере каждые 90 дней.

5.5.2 *Директория открытых ключей (ДОК) ИКАО*

В целях эффективного совместного использования сертификатов лиц, подписывающих документы (C_{DS}), всех государств ИКАО определит и будет предоставлять услуги службы Директории открытых ключей (ДОК) всем участвующим государствам. Эта служба БУДЕТ принимать информацию об открытых ключах государств, хранить их в Директории и делать их доступной для всех других государств.

Доступ для *обновления* списков сертификатов, хранящихся в ДОК, ПРЕДОСТАВЛЯЕТСЯ только участвующим государствам.

Контроль за доступом для *считывания* ДОК (например, с целью скачивания информации ДОК) НЕ ОСУЩЕСТВЛЯЕТСЯ.

Сертификаты подписывающегося СА страны

Сертификаты подписывающегося СА страны (C_{CSCA}) не являются частью услуг ДОК ИКАО. Однако ДОК ИСПОЛЬЗУЕТ сертификаты подписывающегося СА страны (C_{CSCA}) для верификации подлинности и целостности получаемых от участвующих государств сертификатов лиц, подписывающих документы (C_{DS}), перед их опубликованием.

ИКАО не предоставляет доступ к сертификату подписывающегося СА страны (C_{CSCA}).

Сертификаты лиц, подписывающих документы

ДОК ИКАО предназначена быть репозитарием всех сертификатов лиц, подписывающих документы (C_{DS}), используемых в любое время всеми участвующими государствами. Они включают сертификаты, активно используемые в любое время для целей подписания, а также уже не используемые, но еще действительные сертификаты на все выданные МСОПД.

ДОК ИКАО будет *основным* механизмом распределения всех сертификатов лиц, подписывающих документы (C_{DS}), и, следовательно, ДОЛЖНА пополняться и обновляться всеми участвующими государствами.

Информация об открытых ключах какого-либо государства выдачи, хранящаяся в ДОК ИКАО, также ПРЕДОСТАВЛЯЕТСЯ другим сторонам (помимо государств-участников), нуждающимся в такой информации для валидации аутентичности данных, хранящихся в МСОПД в цифровой форме.

Списки отзыва сертификатов

ДОК будет также служить репозитарием всех списков отзыва сертификатов (CRL), выпущенных каждым участвующим государством. Хотя государства в первую очередь РАССЫЛАЮТ CRL друг другу, тем не менее, они ДОЛЖНЫ также посылать их ДОК. Таким образом, ДОК будет *вторичным* механизмом рассылки CRL.

5.5.3 *Принимающие государства*

Пользователи ДОК ИМЕЮТ доступ к услугам ДОК ИКАО на регулярной основе и могут скачивать новую информацию о сертификатах ключей для хранения и использования их внутренними системами пограничного контроля.

Таким образом, обязанностью принимающего государства является поддержание хэш-памяти текущих CRL, а именно текущего набора CRL, который ЯВЛЯЕТСЯ частью скачиваемой из ДОК ИКАО информации.

Каждое принимающее государство ОБЕСПЕЧИВАЕТ внутреннюю рассылку сертификатов подписывающегося СА страны (C_{CSCA}), сертификатов лиц, подписывающих документы (C_{DS}) и CRL в своей системе проверки.

Обязанностью государства является надежное хранение сертификатов подписывающегося СА страны (C_{DS}), как предметов доверия, в своих системах пограничного контроля.

5.5.4 *Другие стороны*

Каждый, кто имеет соответствующее оборудование, может считывать содержание бесконтактных ИС МСОПД, однако лишь стороны, обладающие соответствующими сертификатами открытых ключей и листами отзыва сертификатов, будут иметь возможность верифицировать аутентичность и целостность содержания бесконтактных ИС. Эти стороны МОГУТ получать эту информацию из Директории открытых ключей ИКАО, однако набор сертификатов подписывающегося СА страны (C_{CSCA}) они должны будут получать при помощи других средств, так как они не публикуются в ДОК ИКАО.

5.6 Аутентификация данных

5.6.1 *Пассивная аутентификация*

Помимо групп данных LDS бесконтактная ИС содержит также объект защиты документа (SO_D). Этот объект подписывается в цифровой форме государством выдачи и содержит хэшированное представление содержания LDS (см. п. 7 настоящего раздела).

Система проверки, содержащая открытый ключ лица, подписывающего документы (KPu_{DS}), каждого государства, или считавшая с МСОПД сертификат лица, подписывающего документы (C_{DS}), может верифицировать объект защиты документа (SO_D). Таким способом через содержание объекта защиты документа (SO_D) производится аутентификация содержания LDS.

Этот механизм верификации не требует использования процессорных возможностей бесконтактной ИС МСОПД. В этой связи он называется "пассивной аутентификацией" содержания бесконтактной ИС.

Пассивная аутентификация доказывает, что содержание объекта защиты документа (SO_D) и LDS является подлинным и не было изменено. Она не предотвращает точное копирование содержания бесконтактной ИС или ее подмену.

Следовательно, систему пассивной аутентификации СЛЕДУЕТ поддерживать дополнительной физической проверкой МСОПД.

Пассивная аутентификация определяется в п. 7.2.2.

5.6.2 *Активная аутентификация*

Государство выдачи МОЖЕТ пожелать защитить свои МСОПД от подмены бесконтактной ИС. Это может быть сделано путем внедрения механизма активной аутентификации.

Если механизм активной аутентификации поддерживается, то посредством запросно-ответного протокола между системой проверки и бесконтактной ИС МСОПД он ДОЛЖЕН обеспечивать невозможность подмены бесконтактной ИС.

С этой целью бесконтактная ИС содержит собственную пару ключей активной аутентификации (KPr_{AA} и KPu_{AA}). Хэшированное представление группы данных 15 (информация об открытом ключе (KPu_{AA})) хранится в объекте защиты документа (SO_D) и, следовательно, аутентифицируется цифровой подписью выдающего лица. Соответствующий закрытый ключ (KPr_{AA}) хранится в защищенной памяти бесконтактной ИС.

Путем аутентификации визуальной МСЗ (через хэшированную МСЗ в объекте защиты документа (SO_D)) в сочетании с запросом-ответом система проверки, используя пару ключей активной аутентификации (KPr_{AA} и KPu_{AA}) МСОПД, подтверждает, что объект защиты документа считан с подлинной бесконтактной ИС, хранящейся в подлинном МСОПД.

Активная аутентификация требует использования процессорных возможностей бесконтактной ИС МСОПД.

Активная аутентификация определяется в п. 7.2.2.

5.7 Контроль доступа

Сравнение МСОПД, оснащенного бесконтактной ИС, с обычным МСОПД, свидетельствует о двух различиях:

- Хранящиеся на бесконтактной ИС данные можно считать с помощью электронного устройства без разрешения на считывание документа (скимминг).

- Обмен нешифрованными данными между бесконтактной ИС и считывающим устройством может быть перехвачен с расстояния в несколько метров.

Несмотря на наличие возможных мер физической защиты от скимминга, они не решают проблемы перехвата. В этой связи предполагается, что государства МОГУТ пожелать внедрить механизм базового контроля доступа, т. е. механизм контроля доступа, фактически требующий, чтобы владелец МСОПД знал о том, что хранящиеся на бесконтактной ИС данные, считываются безопасным способом. Такой механизм базового контроля доступа предотвращает скимминг, а также перехват.

Эта рекомендуемая передовая практика призвана защищать частную жизнь и уважать права пассажиров на такую защиту посредством предотвращения скимминга и перехвата.

Этот механизм контроля доступа является ФАКУЛЬТАТИВНЫМ. Содержащиеся в настоящем разделе описание и спецификации, касающиеся базового контроля доступа и безопасного обмена сообщениями, применяются только к МСОПД и системам проверки, поддерживающим этот вариант. Если данный механизм поддерживается, он ДОЛЖЕН обеспечивать возможность считывания содержания бесконтактной ИС только после сознательного предоставления МСОПД его владельцем.

Бесконтактная ИС, защищенная механизмом базового контроля доступа, отказывает в предоставлении доступа к своему содержанию, если система проверки не может доказать, что ей разрешен доступ к бесконтактной ИС. Это доказательство предоставляется по запросно-ответному протоколу, в соответствии с которым система проверки доказывает знание индивидуальных базовых ключей доступа к документу на бесконтактной ИС (K_{ENC} и K_{MAC}), которые извлекаются из информации в МСЗ.

Система проверки ДОЛЖНА быть обеспечена этой информацией до считывания бесконтактной ИС. Данная информация снимается оптически/визуально с МСОПД (например с МСЗ). Проверяющий ДОЛЖЕН также иметь возможность ввести эту информацию в систему проверки вручную в случае невозможности машинного считывания МСЗ.

Кроме того, после успешной аутентификации системой проверки, ТРЕБУЕТСЯ, чтобы бесконтактная ИС обеспечила шифрование канала передачи данных между системой проверки и бесконтактной ИС МСОПД методом безопасного обмена сообщениями.

Предположение о том, что базовые ключи доступа к документу (K_{ENC} и K_{MAC}) не могут быть получены с нераскрытого документа (поскольку они извлекаются из оптически считываемой МСЗ), позволяет допускать, что МСОПД сознательно предоставлен для проверки. Ввиду шифрования канала перехват передаваемых сообщений требует значительных усилий.

Механизм контроля доступа определяется в п. 7.2.2.

5.8 Защита дополнительных биометрических параметров

Персональными данными, хранящимися на бесконтактной ИС, которые определяются как обязательный минимум для обеспечения глобальной интероперабельности, являются МСЗ и изображение лица владельца, хранящееся в цифровой форме. Оба элемента могут также просматриваться (считываться) визуально после того, как МСОПД открыт и предоставлен для проверки.

Помимо хранящегося цифрового изображения лица, как основного биометрического параметра для обеспечения глобальной интероперабельности, ИКАО одобряет использование хранящихся цифровых изображений пальцев и/или радужной оболочки глаза в дополнение к изображению лица. Для внутреннего или двустороннего использования государства МОГУТ предпочесть хранить шаблоны и/или МОГУТ ограничивать доступ или шифровать эти данные, и такое решение принимается самими государствами.

Доступ к этим более конфиденциальным персональным данным СЛЕДУЕТ ограничивать в большей степени. Это может делаться двумя способами: расширением контроля доступа или шифрованием данных. Хотя эти варианты упоминаются в этом разделе, ИКАО в настоящее время не предлагает и не определяет каких-либо стандартов или практических методов в этих сферах.

5.8.1 *Расширенный контроль доступа*

Механизм ФАКУЛЬТАТИВНОГО расширенного контроля доступа аналогичен уже описанному механизму базового контроля доступа, однако для расширенного контроля доступа используется набор расширенных ключей контроля доступа к документу вместо базовых ключей контроля доступа к документу (K_{ENC} и K_{MAC}).

Определение (индивидуального для бесконтактной ИС) набора расширенных ключей доступа к документу производится по усмотрению внедряющего государства. Набор расширенных ключей доступа к документу МОЖЕТ состоять либо из симметричных ключей (например, полученных из МСЗ и национального мастер-ключа) или из пары ассиметричных ключей с соответствующим верифицируемым карточкой сертификатом.

Расширенный контроль доступа требует использования процессорных возможностей бесконтактной ИС МСОПД.

5.8.2 *Шифрование*

Ограничение доступа к дополнительным биометрическим параметрам МОЖЕТ также производиться путем их шифрования. Чтобы иметь возможность расшифровать зашифрованные данные, система проверки ДОЛЖНА обеспечиваться ключом дешифрования. Определение

алгоритма шифрования/расшифровки и ключей, подлежащих использованию, осуществляется по усмотрению внедряющего государства и выходит за рамки настоящего документа.

6. ЗАЩИТА ЭЛЕКТРОННЫХ ДАННЫХ В МСОПД (РЕЗЮМЕ)

Помимо пассивной аутентификации с помощью цифровых подписей государства МОГУТ выбрать дополнительные средства обеспечения безопасности с использованием более сложных способов защиты бесконтактной ИС и ее данных. Варианты, приводимые в таблице IV-1, могут быть надлежащим образом объединены в целях усиления защиты в соответствии с действующими стандартами ИСО/МЭК.

Таблица IV-1. Защита электронных данных (резюме)

Метод	Выдающий орган	Система проверки	Преимущества	Недостатки
БАЗОВЫЙ МЕТОД ЗАЩИТЫ				
Пассивная аутентификация (5.6.1)	**M**	**M**	Доказывает, что содержание SO_D и LDS является подлинным и не изменено	Не предотвращает точное копирование или подмену ИС. Не предотвращает несанкционированный доступ. Не предотвращает скимминг
УСОВЕРШЕНСТВОВАННЫЕ МЕТОДЫ ЗАЩИТЫ				
Сравнение обычной МСЗ (OCR-B) и МСЗ (LDS), базирующейся на ИС	N/A	O	Доказывает, что содержание бесконтактной ИС и физического МСОПД соответствуют друг другу	Вносит (незначительную) сложность. Не предотвращает точное копирование бесконтактной ИС и обычного документа
Активная аутентификация (5.6.2)	O	O	Предотвращает копирование SO_D и доказывает, что он считан с аутентичной бесконтактной ИС. Доказывает, что бесконтактная ИС не подменена	Вносит сложность. Требует использования процессора ИС
Базовый контроль доступа (5.7)	O	O	Предотвращает скимминг и злоупотребление. Предотвращает перехват обмена сообщениями между МСОПД и проверочной системой (при использовании для установки зашифрованного канала передачи)	Не предотвращает точное копирование или подмену бесконтактной ИС (требует также копирования обычного документа). Вносит сложность. Требует использования процессора ИС
Расширенный контроль доступа (5.8.1)	O	O	Предотвращает несанкционированный доступ к дополнительным биометрическим параметрам. Предотвращает скимминг дополнительных биометрических параметров	Требует дополнительного управления ключами. Не предотвращает точное копирование или подмену бесконтактной ИС (требует также копирования обычного документа). Вносит сложность. Требует использования процессора ИС
Шифрование данных (5.8.2)	O	O	Защищает дополнительные биометрические параметры. Не требует использования процессора ИС	Требует сложного управления ключами шифрования. Не предотвращает точное копирование или подмену бесконтактной ИС. Вносит сложность

МСОПД, выдаваемые государствами, решившими использовать усовершенствованные методы защиты, будут полностью совместимы с требованиями ИКАО и считаться отвечающими стандартам глобальной интероперабельности.

7. СПЕЦИФИКАЦИИ

7.1 Изготовление и персонализация МСОПД

7.1.1 Изготовление и персонализация МСОПД являются обязанностью государства выдачи.

Однако государствам РЕКОМЕНДУЕТСЯ принимать меры по обеспечению безопасности транспортировки и хранения бесконтактных ИС, заделывания бесконтактных ИС в МСОПД и процесса их персонализации.

Настоящее издание тома 2 части 3 документа Doc 9303 базируется на предположении о том, что в МСОПД после персонализации записи вноситься не будут. Поэтому в качестве заключительного шага в процессе персонализации бесконтактную ИС СЛЕДУЕТ блокировать. После того, как бесконтактная ИС заблокирована (после персонализации и перед выдачей), больше никаких данных на нее не вносится, а имеющиеся данные на бесконтактной ИС не изменяются и не удаляются. Заблокированную бесконтактную ИС невозможно разблокировать после выдачи документа.

В случае отсутствия в государстве инфраструктуры PKI, необходимой для подписания данных МСОПД как части персонализации, и невозможности задержки выдачи документа(ов), бесконтактную ИС МСОПД РЕКОМЕНДУЕТСЯ оставлять пустой и блокировать. В МСОПД СЛЕДУЕТ напечатать соответствующее предупреждение на этот счет. Предполагается, что это будет исключительным обстоятельством.

7.1.2 *Информация, хранящаяся на бесконтактной ИС*

Схематически содержание бесконтактной ИС МСОПД следующее:

MF	
|	
|---------DF — LDS	ОБЯЗАТЕЛЬНЫЙ
|	
|---------K_{ENC}	ФАКУЛЬТАТИВНЫЙ
|	
|---------K_{MAC}	ФАКУЛЬТАТИВНЫЙ
|	
|---------KPr_{AA}	ФАКУЛЬТАТИВНЫЙ
|	
|---------EF — COM	ОБЯЗАТЕЛЬНЫЙ
|	
|---------EF — SO_D	ОБЯЗАТЕЛЬНЫЙ
|	
|---------EF — Группа данных_1 (МСЗ)	ОБЯЗАТЕЛЬНЫЙ
|	
|---------EF — Группа данных_2 (Закодированное изображение лица)	ОБЯЗАТЕЛЬНЫЙ
//	
|---------EF — Группа данных_n	ФАКУЛЬТАТИВНЫЙ

K_{ENC} , K_{MAC}

Базовые ключи доступа к документу (K_{ENC} и K_{MAC}) (ФАКУЛЬТАТИВНЫЕ) хранятся в DF. Получение этих ключей из МСЗ описывается в добавлении 5.

KPr_{AA}

Закрытый ключ активной аутентификации (KPr_{AA}) (ФАКУЛЬТАТИВНЫЙ) хранится в DF.

EF-COM

См. раздел III, *LDS.*

EF—группа данных 1-n

См. раздел III, *LDS.*

EF-SO_D

Файл EF-SO_D содержит объект защиты документа (SO_D). Объект защиты документа (SO_D) содержит хэш-значения используемых групп данных LDS. (Эта структура называется объектом защиты LDS (SO_{LDS}.)) Спецификация объекта защиты документа (SO_D), приводится в добавлении 3.

7.2 Проверка

7.2.1 *Система проверки*

В целях обеспечения выполнения требуемых функций и определенных вариантов, внедряемых на предоставляемых МСОПД, система проверки должна удовлетворять некоторым предварительным условиям.

Базовый контроль доступа к МСОПД

Хотя описываемый базовый контроль доступа является ФАКУЛЬТАТИВНЫМ, системы проверки, поддерживающие его, ДОЛЖНЫ удовлетворять следующим предварительным условиям:

1. Система проверки оснащена считывателем МСЗ или каким-либо устройством ручного ввода данных (например клавиатурой) для выведения базовых ключей доступа к документу (K_{ENC} и K_{MAC}) с МСОПД.

2. Программное обеспечение системы проверки поддерживает протокол, описываемый в п. 7.2.2, в случае, когда системе предоставляется МСОПД с базовым контролем доступа, включая шифрование передачи данных с безопасным обменом сообщениями.

Пассивная аутентификация

Для осуществления пассивной аутентификации данных, хранящихся на бесконтактной ИС МСОПД, система проверки должна знать ключевую информацию государств выдачи:

1. Сертификат подписывающегося СА страны (C_{CSCA}) каждого участвующего государства выдачи ХРАНИТСЯ в системе проверки.

2. Сертификат лица, подписывающего документы (C_{DS}), каждого участвующего государства выдачи ХРАНИТСЯ в системе проверки.

Прежде чем использовать сертификат лица, подписывающего документы (CDS) для верификации SOD, проверочная система ВЕРИФИЦИРУЕТ его цифровую подпись, используя открытый ключ подписывающегося СА страны (KPu_{CSCA}).

Активная аутентификация

Поддержка активной аутентификации системами проверки является ФАКУЛЬТАТИВНОЙ.

Если система проверки поддерживает ФАКУЛЬТАТИВНУЮ активную аутентификацию, ТРЕБУЕТСЯ, чтобы система проверки была способна считывать визуальную МСЗ.

Если система проверки поддерживает ФАКУЛЬТАТИВНУЮ активную аутентификацию, то программное обеспечение систем проверки ПОДДЕРЖИВАЕТ протокол активной аутентификации, описание которого приведено в п. 7.2.2.

Расширенный контроль доступа к дополнительным биометрическим параметрам

Осуществление защиты ФАКУЛЬТАТИВНЫХ дополнительных биометрических параметров зависит от внутренних спецификаций государства или спецификаций, согласованных на двусторонней основе между государствами, обменивающимися такой информацией.

Расшифровка дополнительных биометрических параметров

Осуществление защиты ФАКУЛЬТАТИВНЫХ дополнительных биометрических параметров зависит от внутренних спецификаций государства или спецификаций, согласованных на двусторонней основе между государствами, обменивающимися такой информацией.

7.2.2 *Последовательность этапов процесса проверки*

В настоящем пункте описываются этапы процесса проверки в порядке их следования. Дается описание как ФАКУЛЬТАТИВНЫХ, так и ОБЯЗАТЕЛЬНЫХ этапов.

Базовый контроль доступа к МСОПД (ФАКУЛЬТАТИВНЫЙ)

Когда МСОПД с ФАКУЛЬТАТИВНЫМ механизмом базового контроля доступа предоставляется проверочной системе, оптически или визуально считываемая информация используется для выведения базовых ключей доступа к документу (K_{ENC} и K_{MAC}) с целью получения доступа к бесконтактной ИС и установления защищенного канала для обмена данными между бесконтактной ИС МСОПД и проверочной системой.

Бесконтактная ИС МСОПД, поддерживающая базовый контроль доступа, после установления защищенного канала ДОЛЖНА давать на неаутентифицированные попытки считывания (включая выбор (защищенных) файлов в LDS) ответ "Статус защиты неудовлетворителен" (0x6982). Посылка незащищенной команды "SELECT" (выбор) по защищенному каналу приводит к прерыванию защищенного канала. Если незащищенная команда "SELECT" посылается до того, как установлен защитный канал или после прерывания защищенного канала, то оба ответа 6982 и 9000 отвечают требованиям ИКАО.

Для аутентификации системы проверки ДОЛЖНЫ быть выполнены следующие этапы:

1. Система проверки считывает "информацию МСЗ", состоящую из конкатенации номера документа, даты рождения и даты истечения срока действия, включая соответствующие контрольные цифры, как описывается в п. 15 раздела IV и п. 8 раздела V для ПД-1 и п. 8 раздела VI для ПД-2 тома 1 части 3 документа Doc 9303, в машиносчитываемой зоне, используя считыватель знаков в формате OCR-B. В качестве альтернативы нужная информация может впечатываться; в этом случае она ВПЕЧАТЫВАЕТСЯ в том виде, в каком фигурирует в МСЗ. 16 наиболее значимых байтов алгоритма хэширования (SHA-1) этой "информации МСЗ" используются в качестве начального заполнения генератора ключей с целью установить базовые ключи доступа к документу, используя механизм выведения ключей, описываемый в п. A.5.1 добавления 5.

2. Система проверки и бесконтактная ИС МСОПД взаимно аутентифицируются и устанавливают сеансовые ключи. ДОЛЖЕН использоваться протокол аутентификации и установления ключей, описываемый в п. A5.2 добавления 5.

3. После успешной аутентификации последующая передача данных ДОЛЖНА защищаться безопасным обменом сообщениями, который описывается в п. A5.3 добавления 5.

Пассивная аутентификация (ОБЯЗАТЕЛЬНАЯ)

Система проверки выполняет следующие этапы:

1. Объект защиты документа (SO_D) (ФАКУЛЬТАТИВНО содержащий сертификат лица, подписывающего документы (C_{DS})), считывается с бесконтактной ИС.

2. Подпись лица, подписывающего документы (DS), считывается с объекта защиты документа (SO_D).

3. Цифровая подпись объекта защиты документа (SO_D) верифицируется системой проверки с использованием открытого ключа лица, подписывающего документы (KPu_{DS}). Сертификат лица, подписывающего документы (C_{DS}), для этого ключа хранится в системе проверки, в качестве скаченной из ДОК ИКАО информации, и также МОЖЕТ храниться на бесконтактной ИС МСОПД. Это гарантирует, что объект защиты документа (SO_D) является аутентичным и что он выдан полномочным органом, упомянутым в объекте защиты документа (SO_D), и не изменен. Следовательно, содержанию объекта защиты документа (SO_D) можно доверять и его СЛЕДУЕТ использовать в процессе проверки. Прежде чем использовать сертификат лица, подписывающего документы (CDS) для верификации SOD, проверочная система ВЕРИФИЦИРУЕТ его цифровую подпись, используя открытый ключ подписывающегося CA страны (KPu_{CSCA}).

4. Проверочная система считывает соответствующие группы данных с LDS.

5. Путем хэширования содержания и сравнения результата с соответствующим хэш-значением в объекте защиты документа (SO_D) система гарантирует, что содержание группы данных является аутентичным и не изменено.

Теперь биометрическая информация может использоваться для биометрической верификации лица, предъявляющего МСОПД.

Активная аутентификация (факультативная)

Если биометрической системе предоставляется МСОПД с ФАКУЛЬТАТИВНОЙ группой данных 15, МОЖЕТ использоваться механизм активной аутентификации с целью гарантировать, что данные считываются с подлинной бесконтактной ИС и что бесконтактная ИС и страница данных принадлежат друг другу.

Проверочная система и бесконтактная ИС выполняют следующие этапы:

1. Вся МСЗ визуально считывается со страницы данных МСОПД (если она еще не считана в рамках процедуры базового контроля доступа) и сравнивается со значением МСЗ в группе данных 1. Поскольку аутентичность и целостность группы данных 1 проверены посредством пассивной аутентификации, сходство гарантирует, что визуальная МСЗ является аутентичной и не изменена.

2. Пассивная аутентификация также доказала аутентичность и целостность группы данных 15. Это гарантирует, что открытый ключ активной аутентификации (KPu_{AA}) является аутентичным и не изменен.

3. Чтобы гарантировать, что объект защиты документа (SO_D) не является копией, система проверки использует пару ключей активной аутентификации МСОПД (KPr_{AA}. и KPu_{AA}) по запросно-ответному протоколу с бесконтактной ИС МСОПД, как описывается в п. A4.2 добавления 4.

Успешное выполнение запросно-ответного протокола доказывает, что объект защиты документа (SO_D) принадлежит странице данных, бесконтактная ИС является подлинной и бесконтактная ИС и страница данных принадлежат друг другу.

Расширенный контроль доступа к дополнительным биометрическим параметрам (ФАКУЛЬТАТИВНЫМ)

Осуществление защиты ФАКУЛЬТАТИВНЫХ дополнительных биометрических параметров зависит от внутренних спецификаций государства или спецификаций, согласованных на двусторонней основе между государствами, обменивающимися этой информацией.

Расшифровка дополнительных биометрических параметров (ФАКУЛЬТАТИВНЫХ)

Осуществление защиты ФАКУЛЬТАТИВНЫХ дополнительных биометрических параметров зависит от внутренних спецификаций государства или спецификаций, согласованных на двусторонней основе между государствами, обменивающимися этой информацией.

7.2.3 *Дополнительный набор команд*

Минимальный набор команд (определен в разделе III) ДОЛЖЕН по крайней мере содержать команды:

SELECT (см. ИСО/МЭК 7816-4),
READ BINARY (см. ИСО/МЭК 7816-4).

Выполнение рекомендаций, которые в настоящем разделе определяются как ФАКУЛЬТАТИВНЫЕ, требует поддержки следующих дополнительных команд:

EXTERNAL AUTHENTICATE (см. ИСО/МЭК 7816-4),
INTERNAL AUTHENTICATE (см. ИСО/МЭК 7816-4),
GET CHALLENGE (см. ИСО/МЭК 7816-4).

8. АЛГОРИТМЫ

8.1 Обзор

Государства ДОЛЖНЫ поддерживать один и тот же алгоритм для использования в своих подписывающихся СА страны, ключах подписи документов и, где это применимо, парах ключей активной аутентификации, несмотря на то, что могут требоваться различные размеры ключей в зависимости от выбранного алгоритма.

Государства ДОЛЖНЫ поддерживать все алгоритмы в пунктах, где они желают проверять подлинность подписи на документах в виде МСОПД и где они обмениваются информацией об управлении ключами с другими государствами.

Содержащиеся здесь рекомендации о размерах ключей предполагают максимальные рекомендации в отношении периодов выдачи ключей и максимальный десятилетний срок действия документа.

Для генерирования подписи в механизме активной аутентификации государства используют стандарт ИСО/МЭК 9796-2, 2002 г., *"Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений", часть 2 "Механизмы на основе целочисленной факторизации*".

Для использования в своих подписывающихся СА страны, ключах подписи документов и, где применимо, объектах защиты документов, государства ПОДДЕРЖИВАЮТ один из нижеуказанных алгоритмов.

8.2 RSA

Государства, применяющие алгоритм RSA для генерирования подписи и верификации сертификатов и объекта защиты документа (SO_D), ИСПОЛЬЗУЮТ документ *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003).* В RFC 3447 определены два механизма подписи: RSASSA-PSS и RSASSA-PKCS1_v15. Подписи РЕКОМЕНДУЕТСЯ генерировать в соответствии с RSASSA-PSS, но принимающие государства ДОЛЖНЫ также быть готовы верифицировать подписи, соответствующие RSASSA-PKCS1_v15.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модуля n для ключей подписывающегося СА страны, использующих RSA, составлял *3072 бит*.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модуля n для ключей лица, подписывающего документы, использующих RSA, составлял *2048 бит*.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модуля n для ключей активной аутентификации, использующих RSA, составлял *1024 бит*.

8.3 Алгоритм цифровой подписи (DSA)

Государства, реализующие алгоритм DSA для генерирования или верификации подписей, ИСПОЛЬЗУЮТ стандарт *FIPS 186-2, Публикация Федеральных стандартов обработки информации (FIPS PUB) 186-2 (+ Change Notice), Стандарт цифровой подписи, 27 января 2000 г. (Заменяет FIPS PUB 186-1 от 15 декабря 1998 г.)).*

Действующие спецификации FIPS 186-2 для DSA поддерживают только длину ключа 1024. Новый вариант стандарта FIPS 186-3 проходит испытания, однако дату его готовности в настоящее время определить невозможно.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модулей p и q для ключей подписывающегося СА страны, использующих DSA, составлял *3072 и 256 бит* соответственно.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модулей p и q для ключей лица, подписывающего документы, использующих DSA, составлял *2048 и 224 бит* соответственно.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер модулей p и q для ключей активной аутентификации, использующих DSA, составлял *1024 и 160 бит* соответственно.

8.4 DSA с эллиптической кривой

Государства, применяющие алгоритм ECDSA для генерирования или верификации подписи, ИСПОЛЬЗУЮТ стандарт X9.62 ([R11], *X9.62, “Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 7 January 1999 или ИСО/МЭК 15946 "Методы криптографии на основе эллиптических кривых, 2002 г.").* Параметры области эллиптической кривой, используемые для генерирования пары ключей ECDSA, ДОЛЖНЫ быть ясно описаны в параметрах открытого ключа, т. е. параметры ДОЛЖНЫ быть типа EC параметров (без наименованных кривых, без подразумеваемых параметров) и ДОЛЖНЫ включать факультативный сопутствующий фактор. EC точки ДОЛЖНЫ быть в несжатом формате.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер для последовательности базовых точек для ключей подписывающегося СА страны, использующих ECDSA, составлял *256 бит*.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер для последовательности базовых точек для ключей лица, подписывающего документы, использующих ECDSA, составлял *224 бит*.

РЕКОМЕНДУЕТСЯ, чтобы минимальный размер для последовательности базовых точек для ключей активной аутентификации, использующих ECDSA, составлял *160 бит*.

8.5 Алгоритмы хэширования

SHA-1, SHA-224 (проект), SHA-256, SHA-384 и SHA-512 являются разрешенными алгоритмами хэширования. См.*FIPS 180-2, Публикация Федеральных стандартов обработки информации (FIPS PUB) 180-2, Стандарт хэширования в целях защиты, август 2002 г.*

Для выбранного алгоритма подписи СЛЕДУЕТ отобрать алгоритм хэширования соответствующего размера. Например:

- SHA-1 с RSA 1024;
- SHA-224 с ECDSA 224.

9. УПРАВЛЕНИЕ КЛЮЧАМИ

9.1 Обзор

Государства выдачи ДОЛЖНЫ иметь по крайней мере два типа ключей, которые именуются:

- ключи подписывающегося СА страны,
- ключи лиц, подписывающих документы.

Государства выдачи МОГУТ иметь дополнительные типы ключей:

- ключи активной аутентификации.

Ключи подписывающегося СА страны и ключи лиц, подписывающих документы, выдаются с использованием сертификатов X.509 *(см. RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002),* а открытые ключи, содержащиеся в них, используются для валидации ключей лиц, подписывающих документы (в случае использования ключей подписывающегося СА страны), или объектов защиты документов (SO_D), выдаваемых этим государством (в случае использования ключей лиц, подписывающих документы).

Все сертификаты, выдаваемые государствами, ДОЛЖНЫ соответствовать профилю сертификата, указанному в добавлении 1.

Государства ДОЛЖНЫ периодически выпускать список отзыва сертификатов; см. п. 9.5, касающийся отзыва сертификатов.

9.2 Ключи активной аутентификации

ФАКУЛЬТАТИВНЫЕ пары ключей активной аутентификации (KPr_{AA}. и KPu_{AA}) ГЕНЕРИРУЮТСЯ безопасным способом.

Открытый ключ активной аутентификации (KPu_{AA}) и закрытый ключ активной аутентификации (KPr_{AA}.) вносятся в бесконтактную ИС МСОПД. После этого процедура управления ключами не применяется к этим ключам.

9.3 Ключи лиц, подписывающих документы

Сертификаты лиц, подписывающих документы (C_{DS}), используются для верификации действительности объектов защиты документа (SO_D). Поэтому для принятия электронного МСОПД другого государства принимающее государство ДОЛЖНО предварительно поместить в определенное доверительное хранилище копии исходящих сертификатов лиц, подписывающих документы (C_{DS}).

Сертификат лица, подписывающего документы (C_{DS}), РЕКОМЕНДУЕТСЯ хранить в объекте защиты документа (SO_D). См. добавление 3.

Сертификат лица, подписывающего документы (C_{DS}), может считываться с бесконтактной ИС МСОПД, если государство выдачи обеспечивает хранение этого сертификата на бесконтактной ИС.

Срок службы ключа лица, подписывающего документы

Срок службы (т. е. период действия сертификата) ключа лица, подписывающего документы, определяется путем конкатенации следующих двух периодов:

- продолжительность времени использования ключа для выдачи МСОПД и
- срок действия [наиболее длительный] любого МСОПД, выданного под этим ключом.[1]

Сертификат лица, подписывающего документы (C_{DS}), ДЕЙСТВИТЕЛЕН в течение всего этого периода, чтобы можно было осуществлять верификацию подлинности МСОПД. Однако ключ СЛЕДУЕТ использовать только для выдачи документов на ограниченный период времени; по истечении срока действия последнего документа, для выдачи которого он использовался, открытый ключ больше не требуется.

После выдачи последнего документа государствам РЕКОМЕНДУЕТСЯ стирать закрытый ключ поддающимся проверке и учету способом.

Период выдачи ключа лица, подписывающего документы

При развертывании своих систем государства могут пожелать учитывать количество документов, которые будут подписываться каким-либо одним индивидуальным ключом лица, подписывающего документы. Государство, ежедневно выдающее большое количество документов и использующее только один ключ лица, подписывающего документы, может пожелать использовать короткий период выдачи для сокращения эксплуатационных расходов по обеспечению непрерывности в случае отзыва ключа лица, подписывающего документы (см. п. 9.5). В качестве альтернативы государство может также пожелать использовать большое количество ключей подписи для сокращения накладных расходов на любой отдельный ключ.

Однако если государство выдает лишь небольшое количество сертификатов, потребности в таком коротком периоде выдачи ключа лица, подписывающего документы, нет и, следовательно, он МОЖЕТ быть более продолжительным.

В этой связи РЕКОМЕНДУЕТСЯ, чтобы максимальный период выдачи ключа лица, подписывающего документы, для подписи МСОПД составлял три месяца. Для государств,

1. Некоторые государства могут выдавать МСОПД до того, как они становятся действительными, например, при смене фамилии после вступления в брак. В результате этого срок действия увеличивается на самый продолжительный период, возможный для предварительной выдачи МСОПД.

изготавливающих большое количество МСОПД, в любой нужный момент МОЖЕТ выпускаться несколько ключей подписи находящихся в обращении документов.

9.4 Ключи подписывающегося СА страны

Сертификаты подписывающегося СА страны (C_{CSCA}) используются для верификации действительности ключей лиц, подписывающих документы. Поэтому для принятия электронного МСОПД другого государства принимающее государство ДОЛЖНО предварительно поместить в какое-либо доверительное хранилище, доступное его системе пограничного контроля, копию исходящего из государства сертификата подписывающегося СА страны (C_{CSCA}).

Срок службы ключа подписывающегося СА страны

Срок службы (т. е. период действия сертификата) ключа подписывающегося СА страны определяется путем конкатенации следующих периодов:

- промежуток времени, в течение которого ключ подписывающегося СА страны будет использоваться для выдачи сертификатов лиц, подписывающих документы (C_{DS});
- срок службы ключей лиц, подписывающих документы, состоящий из:
  - промежутка времени, в течение которого ключ будет использоваться для выдачи МСОПД;
  - наиболее продолжительного периода действия любого МСОПД, выданного под этим ключом.

Период выдачи ключа подписывающегося СА страны

Период выдачи ключа подписывающегося СА страны представляет собой тонкий баланс между следующими факторами:

- В маловероятном случае компрометации государственного ключа подписывающегося СА страны действительность всех МСОПД, выданных с использованием ключей лиц, подписывающих документы, выданных под данным ключом подписывающегося СА страны, подвергается сомнению. В этой связи государства МОГУТ пожелать выдерживать довольно короткий период выдачи.
- Однако выдерживание очень короткого периода выдачи ведет к наличию весьма большого количества ключей подписывающегося СА страны в определенный момент времени. Это может усложнить управление сертификатами в пограничных системах обработки.
- Если смена ключа подписывающегося СА страны будет осуществляться слишком редко, то вполне возможно, что государствам будет сложно делать это из-за нехватки знаний или средств.

В этой связи государственный ключ подписывающегося СА страны РЕКОМЕНДУЕТСЯ менять каждые три-пять лет.

Замена ключа подписи страны

Ключи подписывающегося CA страны являются предметами доверия во всей системе, без которых система разрушится. Поэтому государствам СЛЕДУЕТ тщательно планировать замену своих ключей подписывающегося CA страны. По истечении первоначального периода подписания государство всегда должно будет иметь по крайней мере два одновременно действующих сертификата подписывающегося CA страны (C_{CSCA}).

Государства ДОЛЖНЫ за 90 дней уведомлять о предстоящей замене своих сертификатов CSCA и затем в двустороннем порядке рассылать свои новые сертификаты CSCA. Для аутентификации своих новых сертификатов государствам следует также подтверждать свои новые сертификаты CSCA, используя внеполосный метод.

Государства МОГУТ дополнительно производить связующие сертификаты для обратной поддержки совместимости с ранее выданными сертификатами CSCA. В тех случаях, когда государства решают выдавать связующие сертификаты, им нет необходимости выдавать сертификаты CSCA с использованием внеполосного метода.

Государствам следует воздерживаться от использования своих сертификатов CSCA в первые два дня после выдачи.

9.5 Отзыв сертификатов

Все национальные полномочные органы, выдающие сертификаты лиц, подписывающих документы (C_{DS}), ДОЛЖНЫ периодически готовить информацию в виде списков отзыва сертификатов (CRL). Выпущенные CRL ДОЛЖНЫ соответствовать профилю, определенному в добавлении 2.

Государства ДОЛЖНЫ выпускать по крайней мере один CRL каждые 90 дней. Государства МОГУТ выпускать CRL чаще, чем каждые 90 дней, но не чаще, чем каждые 48 ч.

Уведомление об отзыве

Если государство желает отозвать ключ лица, подписывающего документы, для выпуска нового CRL ему не надо ждать до тех пор, пока истечет очередной период обновления текущего CRL. Новый CRL РЕКОМЕНДУЕТСЯ выпускать в течение 48 ч с момента уведомления об отзыве.

Отзыв ключа подписывающегося CA страны

Отзыв ключа подписывающегося CA страны является одновременно крайней и сложной мерой. После информирования соответствующего государства об отзыве ключа подписывающегося CA страны все другие ключи, выданные с использованием этого ключа, фактически отзываются.

Если государство использовало старый ключ подписывающегося CA страны для аутентификации нового ключа подписывающегося CA страны (см. п. 9.4 "Замена ключа подписи страны"), отзыв старого ключа подписывающегося CA страны ВЛЕЧЕТ за собой также отзыв нового ключа подписывающегося CA страны.

Для выдачи новых документов выдающее государство в сущности ДОЛЖНО снова вернуться к начальной загрузке своего процесса аутентификации путем двустороннего установления

новых сертификатов подписывающегося CA страны (C_{CSCA}), выданных с использованием внеполосного метода.

10. РАССЫЛКА СЕРТИФИКАТОВ И CRL

Государствам необходимо планировать свои стратегии смены сертификатов как для ключей подписывающегося CA страны, так и для ключей лиц, подписывающих документы, с целью обеспечения своевременной передачи сертификатов и CRL в системы пограничного контроля принимающих государств. В идеальном случае, передача будет происходить в течение 48 ч, однако некоторые принимающие государства могут иметь удаленные и плохо подключенные пограничные посты, для передачи сертификатов и CRL в которые может требоваться больше времени. Принимающим государствам СЛЕДУЕТ делать все возможное для рассылки сертификатов и CRL всем пограничным пунктам в течение 48 ч.

Рассылка сертификатов подписывающегося CA страны

Государствам выдачи следует ожидать, что сертификаты подписывающегося CA страны (C_{CSCA}) будут распространяться принимающими государствами в течение 48 ч.

Рассылка сертификатов лиц, подписывающих документы

Государствам выдачи следует ожидать, что сертификаты лиц, подписывающих документы (C_{DS}), будут распространяться принимающими государствами в течение 48 ч.

Государства выдачи могут обеспечивать своевременное распространение сертификатов лиц, подписывающих документы (C_{DS}), путем включения таких сертификатов в объекты защиты документов (SO_D).

Рассылка CRL

Государствам СЛЕДУЕТ делать все возможное, используя либо электронные, либо другие средства, для предпринятия действий по CRL, выпущенным в исключительных обстоятельствах.

10.1 Рассылка через ДОК ИКАО

Основным каналом распределения сертификатов лиц, подписывающих документы (C_{DS}), будет Директория открытых ключей ИКАО. Для CRL ДОК будет вспомогательным каналом. Сертификаты подписывающегося CA страны (C_{CSCA}) не публикуются и не доступны в ДОК, однако они используются ДОК для верификации сертификатов лиц, подписывающих документы (C_{DS}), представленных в нее для опубликования.

Связь

Вся связь с Директорией открытых ключей ИКАО БАЗИРУЕТСЯ на аутентифицированном серверном SSL. С этой целью ИКАО ПОЛУЧАЕТ единый серверный ключ (на каждый сайт) от коммерческой стороны.

Обновление директории

Открытые ключи ПОСЫЛАЮТСЯ в ДОК как сертификаты в формате X.509, подписанные государством выдачи, с использованием ключа подписывающегося CA страны, относящегося к данному государству. Эти сертификаты ОТВЕЧАЮТ требованиям, изложенным в добавлении 1.

Обновление ОСУЩЕСТВЛЯЕТСЯ с использованием протокола LDAP, согласно которому директория меняется в результате пересланных изменений. Ввиду необходимости проявления ИКАО должной осмотрительности в этом процессе, ДОК ДОЛЖНА состоять из "директории для записи", куда посылаются предлагаемые изменения к сертификатам и CRL, и "директории для чтения", которая используется для содержания новых сертификатов, по завершении данного процесса, требующего должной осмотрительности, и доступ к которой предоставляется сообществу пользователей МСОПД для скачивания этой информации.

В силу своего характера сертификаты и CRL подписываются государством выдачи. Эта подпись ВЕРИФИЦИРУЕТСЯ ИКАО перед опубликованием сертификата или CRL в "директории для чтения".

Скачивание директории

ДОК будет создана как директория X.500. Предполагаемый объем ДОК составит 15–20 МБ.

Поскольку ДОК относительно невелика, государствам РЕКОМЕНДУЕТСЯ ежедневно скачивать всю директорию. Это позволит государствам затем обрабатывать эту информацию так, как они хотят.

Доступ к ДОК с правом считывания НЕ ОГРАНИЧИВАЕТСЯ только участвующими государствами. ДОК будет полностью открытым и функционирующим через Интернет ресурсом, доступ к которому только для чтения (скачивания) будет предоставляться также авиакомпаниям и другим подобным сторонам.

10.2 Рассылка с помощью двусторонних средств

Основным каналом распределения CRL и сертификатов подписывающегося CA страны (C_{CSCA}) будет двусторонний обмен между участвующими государствами и государствами-пользователями.

Государства, как правило, имеют двусторонние соглашения и средства взаимного обмена информацией (например, электронная почта или каталог адресов LDAP). Государствам СЛЕДУЕТ использовать эти существующие каналы для обмена сертификатами и CRL.

Государствам, которые в настоящее время не имеют двусторонних соглашений или средств двустороннего обмена информацией, СЛЕДУЕТ заключить такие соглашения и установить такие каналы связи с другими участвующими государствами.

Первоначальный обмен сертификатами подписывающегося CA страны осуществляется по дипломатическим каналам. Это означает, что страны, обменивающиеся сертификатами:

- согласовывают кандидатуры представителей для первоначального обмена ключами;
- определяют подходящий механизм для обмена ключами (например, дипломатическая

почта, или другой существующий надежно защищенный механизм);

- обмениваются сертификатами;

- тестируют сертификаты, используя сертификат лица, подписывающего документ, полученный через отдельный механизм.

Дальнейший обмен сертификатом подписывающегося CA страны между двумя государствами может осуществляться более просто, если при обновлении используются связующие сертификаты.

В добавлении 8 приводится описание механизма получения информации в отношении двустороннего обмена CRL и сертификатами CSCA.

В таблице IV-2 кратко указаны объекты и источники, определяемые в документе Doc 9303 как первичные (primary (P)) и вторичные (secondary (S)).

Таблица IV-2.

	C_{CSCA}	*Null-CRL*	*Non-Null CRL*	C_{DS}
ДОК		S	S	P
Бесконтактная ИС				S
Двусторонний	Только	P	P	

Технически государства не обязаны использовать *оба* источника, т.е. и первичный и вторичный. В процессе повседневной эксплуатации проверочной системы решение о том, использовать ли первичный *или* вторичный источник, принимает проверяющий полномочный орган. Если в своей повседневной деятельности проверяющий полномочный орган использует вторичный источник для сертификата или CRL, тем не менее, ему следует быть готовым поддержать также первичный источник.

ДОБАВЛЕНИЕ 1 (НОРМАТИВНОЕ) к разделу IV

ПРОФИЛЬ СЕРТИФИКАТА

Государства, удовлетворяющие данным техническим условиям, ДОЛЖНЫ выдавать сертификаты, соответствующие этому профилю. Все объекты защиты ДОЛЖНЫ вноситься в формате, определенном в особом правиле кодирования (DER), в целях сохранения целостности содержащихся в них подписей.

Нижеуказанный профиль использует для каждого поля в сертификате X.509 следующую терминологию:

m обязательное (mandatory) – поле ДОЛЖНО присутствовать,
x не использовать – поле НЕ СЛЕДУЕТ заполнять,
o факультативное (optional) – поле МОЖЕТ присутствовать,
c критическое (critical) – обозначение критического расширения; принимающие прикладные программы ДОЛЖНЫ быть способны обрабатывать это расширение.

A1.1 Основная часть сертификата

Компонент сертификата	**Раздел в RFC 3280**	**Сертификат подписывающегося CA страны**	**Сертификат лица, подписывающего документы**	**Замечания**
Сертификат	4.1.1	m	m	
Сертификат TBS	4.1.1.1	m	m	См. следующую часть таблицы
Алгоритм подписи	4.1.1.2	m	m	Вводимое здесь значение зависит от выбранного алгоритма
Значение подписи	4.1.1.3	m	m	Вводимое здесь значение зависит от выбранного алгоритма
Сертификат TBS	4.1.2			
Версия	4.1.2.1	m	m	ДОЛЖНА быть v3
Серийный номер	4.1.2.2	m	m	
Подпись	4.1.2.3	m	m	Вводимое здесь значение ДОЛЖНО соответствовать OID в алгоритме подписи
Выдающий	4.1.2.4	m	m	См. A1.6
Действительность	4.1.2.5	m	m	Ввод в действие ДОЛЖЕН указываться с использованием времени UTC до 2049, а затем с использованием обобщенного времени
Субъект	4.1.2.6	m	m	См. A1.6
Информация об открытом ключе субъекта	4.1.2.7	m	m	

Компонент сертификата	Раздел в RFC 3280	Сертификат подписывающегося CA страны	Сертификат лица, подписывающего документы	Замечания
Уникальная идентификационная информация выдающего	4.1.2.8	x	x	
Уникальная идентификационная информация субъекта	4.1.2.8	x	x	
Расширения	4.1.2.9	m	m	См. следующую таблицу, где указано, какие расширения СЛЕДУЕТ включать

A1.2 Расширения

Название расширения	Раздел в RFC 3280	Сертификат подписывающегося CA страны	Сертификат лица, подписывающего документы	Замечания
Идентификатор ключа полномочного органа	4.2.1.1	o	m	Обязательный во всех сертификатах, за исключением самоподписывающихся сертификатов подписывающегося CA страны
Идентификатор ключа субъекта	4.2.1.2	m	o	
Использование ключа	4.2.1.3	mc	mc	Это расширение ДОЛЖНО обозначаться как КРИТИЧЕСКОЕ
Период использования закрытого ключа	4.2.1.4	o	o	Это будет периодом выдачи закрытого ключа
Политика сертификата	4.2.1.5	o	o	
Отображение политики	4.2.1.6	x	x	
Альтернативное имя субъекта	4.2.1.7	x	x	
Альтернативное имя выдающего	4.2.1.8	x	x	
Атрибуты субъектов директории	4.2.1.9	x	x	
Основные ограничения	4.2.1.10	mc	x	Это расширение ДОЛЖНО обозначаться как КРИТИЧЕСКОЕ
Ограничения в отношении имени	4.2.1.11	x	x	
Ограничения в отношении политики	4.2.1.12	x	x	
Внешнее использование ключей	4.2.1.13	x	x	

Название расширения	**Раздел в RFC 3280**	**Сертификат подписывающегося CA страны**	**Сертификат лица, подписывающего документы**	**Замечания**
Пункты распределения CRL	4.2.1.14	o	o	Если государства решают использовать это расширение, они ДОЛЖНЫ включить ДОК ИКАО в качестве распределительного пункта. Внедрение может также включать относительные CRL DP для местных целей; они могут игнорироваться другими государствами
Любая политика запрета	4.2.1.15	x	x	
Самый свежий CRL	4.2.1.16	x	x	
Частные расширения в Интернете	4.2.2	x	x	
Другие частные расширения	Отсутств.	o	o	При включении любого частного расширения для национальных целей, оно НЕ ДОЛЖНО маркироваться. Государствам не рекомендуется включать никакие частные расширения
Идентификатор ключа полномочного органа	**4.2.1.1**			
Идентификатор ключа		m	m	Если это расширение используется, данное поле ДОЛЖНО как минимум поддерживаться
Лицо, выдающее сертификат полномочного органа		o	o	См. A1.6
Порядковый номер сертификата полномочного органа		o	o	
Идентификатор ключа субъекта	**4.2.1.2**			
Идентификатор ключа субъекта		m	m	
Использование ключа	**4.2.1.3**			
Цифровая подпись		x	m	
Невозможность отрицания		x	x	
Шифрование ключа		x	x	
Шифрование данных		x	x	
Согласование ключа		x	x	
Подпись сертификата ключа		m	x	
Подпись CRL		m	x	
Только шифратор		x	x	

Название расширения	Раздел в RFC 3280	Сертификат подписы-вающегося CA страны	Сертификат лица, подпи-сывающего документы	Замечания
Только дешифратор		x	x	
Основные ограничения	**4.2.1.10**			
cA		m	x	ВЕРНО для сертификатов CA
Ограничение длины пути		m	x	В сертификатах подписывающегося CA страны ограничение длины пути всегда ДОЛЖНО быть "0"
Пункты распределения CRL	**4.2.1.14**			
Пункт распределения		m	x	
Причины		m	x	
Выдающий CRL		m	x	
Политика сертификата	**4.2.1.5**			
Информация о политике				
Идентификатор политики		m	m	
Квалификаторы политики		o	o	

A1.3 Алгоритм подписи

Идентификаторы объекта, определяемые в разделе 2.2 *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", апрель 2002 г.,* и в разделе A.2 *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", февраль 2003 г.*, ИСПОЛЬЗУЮТСЯ для алгоритмов, определенных в п. 8 раздела IV.

A1.4 Значение подписи

Структуры подписи, хранящиеся в поле значения подписи, СООТВЕТСТВУЮТ указанным в разделе 2.2 *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", апрель 2002 г.*, для алгоритмов, определенных в п. 8 раздела IV.

A1.5 Информация об открытом ключе субъекта

Поля информации об открытом ключе субъекта для алгоритмов, определенных в п. 8 раздела IV, ЗАПОЛНЯЮТСЯ в соответствии с разделом 2.3 *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", апрель 2002 г.*

A1.6 Соглашения о сертификатах и именовании

РЕКОМЕНДУЮТСЯ указанные ниже соглашения об именовании и адресации для поля выдающего и поля субъекта в сертификатах CSCA и DS, и для поля выдающего в списках отзыва сертификатов.

СЛЕДУЕТ использовать следующие атрибуты:

- страна (коды страны ДОЛЖНЫ следовать формату двухбуквенных кодов страны, указанных в ИСО/МЭК 3166-1: 2006 г., Коды для представления названий стран и единиц их административно-территориального деления. Часть 1: Коды стран и ИСО 3166-2: 2007 г., Коды для представления названий стран и единиц их административно-территориального деления. Часть 2: Коды единиц административно-территориального деления);

- организация;

- организационное подразделение;

- общее название.

Дополнительно некоторые страны МОГУТ использовать:

- порядковый номер.

Государства, желающие использовать существующие инфраструктуры PKI для поддержки своих систем выдачи МСОПД, могут быть связаны обязательствами по существующим соглашениям об именовании.

ДОБАВЛЕНИЕ 2 (НОРМАТИВНОЕ) к разделу IV

ПРОФИЛЬ CRL

Нижеуказанный профиль использует для каждого поля в списке отзыва сертификатов X.509 следующую терминологию:

m обязательное (mandatory) – поле ДОЛЖНО присутствовать,
x не использовать – поле НЕ СЛЕДУЕТ заполнять,
o факультативное (optional) – поле МОЖЕТ присутствовать,
c критическое (critical) – обозначение критического расширения; принимающие прикладные программы ДОЛЖНЫ быть способны обрабатывать это расширение.

Компонент перечня сертификатов	Раздел в RFC 3280	CRL подписывающегося CA страны	Замечания
Перечень сертификатов	5.1.1	m	
Перечень сертификатов tBS	5.1.1.1	m	См. следующую часть таблицы
Алгоритм подписи	5.1.1.2	m	Вводимое здесь значение зависит от выбранного алгоритма
Значение подписи	5.1.1.3	m	Вводимое здесь значение зависит от выбранного алгоритма
Перечень сертификатов tBS	5.1.2		
Версия	5.1.2.1	m	ДОЛЖНА быть v2
Подпись	5.1.2.2	m	Вводимое здесь значение зависит от выбранного алгоритма
Выдающий	5.1.2.3	m	ТРЕБУЕТСЯ кодирование UTF8
Это обновление	5.1.2.4	m	Ввод в действие ДОЛЖЕН указываться с использованием времени UTC до 2049, а затем с использованием обобщенного времени
Следующее обновление	5.1.2.5	m	Ввод в действие ДОЛЖЕН указываться с использованием времени UTC до 2049, а затем с использованием обобщенного времени
Отозванные сертификаты	5.1.2.6	m	
Расширения crl	5.1.2.7	m	

Название расширения	Раздел в RFC 3280	CRL подписы-вающегося CA страны	Замечания
Идентификатор ключа полномочного органа	5.2.1	m	Это поле ДОЛЖНО иметь то же значение, что и поле идентификатора ключа субъекта в сертификате выдающего CRL
Альтернативное имя выдающего	5.2.2	x	
Номер cRL	5.2.3	m	
Дельта индикатор CRL	5.2.4	x	
Выдающий пункт распределения	5.2.5	x	
Самый свежий CRL	5.2.6	x	
Расширение записей CRL			
Код причины	5.3.1	x	
Код указания о задержке	5.3.2	x	
Дата недействительности	5.3.3	x	
Лицо, выдающее сертификат	5.3.4	x	

Примечание. CRL может содержать другую связанную с отзывом информацию, касающуюся, например, сертификатов оператора системы или полномочного органа регистрации.

ДОБАВЛЕНИЕ 3 (НОРМАТИВНОЕ) к разделу IV

ОБЪЕКТ ЗАЩИТЫ ДОКУМЕНТА

Объект защиты документа реализуется как тип подписываемых данных, указанный в *RFC 3369, Cryptographic Message Syntax, август 2002 г.* Все объекты защиты ВНОСЯТСЯ в формате, определяемом особым правилом кодирования (DER), для сохранения целостности содержащихся в них подписей.

A3.1 Тип подписываемых данных

Применяются правила обработки, содержащиеся в RFC3369.

m обязательное (mandatory) – поле ДОЛЖНО присутствовать,
x не использовать – поле НЕ СЛЕДУЕТ заполнять,
o факультативное (optional) – поле МОЖЕТ присутствовать,
c выбор (choice) – содержание поля выбирается из альтернатив.

Значение		Замечания
Подписываемые данные		
Версия	m	Значение = v3
Алгоритмы представления в краткой форме	m	
Информация об инкапсулированном содержании	m	
Тип электронного содержания	m	id-icao-lds объекта защиты
Электронное содержание	m	Закодированное содержание lds объекта защиты
Сертификаты	o	Государства могут решить включать сертификат лица, подписывающего документы (C_{DS}), который может использоваться для верификации подписи в поле информации о подписавшемся
Crls	x	Государствам рекомендуется не использовать это поле
Информация о подписавшемся	m	Государствам рекомендуется предоставлять в этом поле только одну единицу информации о подписавшемся
Информация о подписавшемся	m	
Версия	m	Значение этого поля диктуется полем sid. См. правила, касающиеся этого поля, в RFC3369, раздел 5.3
Sid	m	
Выдающее лицо и порядковый номер	c	Государствам рекомендуется поддерживать это поле над идентификатором ключа субъекта
Идентификатор ключа субъекта	c	

Значение		Замечания
Алгоритм представления в краткой форме (digest)	m	Алгоритмный идентификатор алгоритма, используемого для выдачи хэш-значения над инкапсулированным содержанием и подписанными атрибутами
Подписанные атрибуты	m	Производящие документы государства могут пожелать включать дополнительные атрибуты для внесения в подпись, однако они должны обрабатываться принимающими государствами только для верификации значения подписи
Алгоритм подписи	m	Алгоритмный идентификатор алгоритма, используемого для выдачи значения подписи и любых связанных с ней параметров
Подпись	m	Результат процесса генерации подписи
Неподписанные атрибуты	o	Производящие документы государства могут пожелать использовать это поле, однако это не рекомендуется, и принимающие государства могут игнорировать их

A3.2 Объект защиты LDS профиля ASN.1

```
LDSSecurityObject    {iso(1)    identified-organization(3)    icao(ccc)    mrtd(1)
security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Imports from RFC 3280 [PROFILE], Appendix A.1
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
id-mod(0) id-pkix1-explicit(18) }

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers
id-icao     OBJECT IDENTIFIER ::= {2.23.136}
id-icao-mrtd   OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security     OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier


LDSSecurityObject ::= SEQUENCE {
      version LDSSecurityObjectVersion,
```

```
      hashAlgorithm DigestAlgorithmIdentifier,
      dataGroupHashValues SEQUENCE SIZE (2..ub-DataGroups) OF
      DataGroupHash }

DataGroupHash ::= SEQUENCE {
      dataGroupNumber         DataGroupNumber,
      dataGroupHashValue      OCTET STRING }

DataGroupNumber ::= INTEGER {
      dataGroup1          (1),
      dataGroup2          (2),
      dataGroup3          (3),
      dataGroup4          (4),
      dataGroup5          (5),
      dataGroup6          (6),
      dataGroup7          (7),
      dataGroup8          (8),
      dataGroup9          (9),
      dataGroup10        (10),
      dataGroup11        (11),
      dataGroup12        (12),
      dataGroup13        (13),
      dataGroup14        (14),
      dataGroup15        (15),
      dataGroup16        (16)}
END
```

Примечание.

Поле `dataGroupValue` содержит вычисленное хэш-значение над *полным* содержанием файла группы данных EF, определяемым номером группы данных.

ДОБАВЛЕНИЕ 4 (НОРМАТИВНОЕ) к разделу IV

АКТИВНАЯ АУТЕНТИФИКАЦИЯ

A4.1 Информация об открытом ключе активной аутентификации

ФАКУЛЬТАТИВНЫЙ открытый ключ активной аутентификации хранится в группе данных 15 LDS. Формат структуры (информация об открытом ключе субъекта) специфицирован в *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, апрель 2002 г*. Все объекты защиты ДОЛЖНЫ вноситься в формате, определенном в особом правиле кодирования (DER), в целях сохранения целостности содержащихся в них подписей.

Информация об открытом ключе активной аутентификации ::= информация об открытом ключе субъекта:

```
SubjectPublicKeyInfo ::= SEQUENCE {
        algorithm           AlgorithmIdentifier,
        subjectPublicKey    BIT STRING }

AlgorithmIdentifier ::= SEQUENCE {
        algorithm           OBJECT IDENTIFIER,
        parameters          ANY DEFINED BY algorithm OPTIONAL }
```

A4.2 Механизм активной аутентификации

Активная аутентификация производится с использованием команды INTERAL AUTHENTICATE (ИСО/МЭК 7816). Для этого вводится специальный идентификатор (Nonce) (RND.IFD), который ДОЛЖЕН составлять 8 байтов. В тех случаях, когда используется механизм на основе целочисленной факторизации ICC вычисляет подпись в соответствии с *ИСО/МЭК 9796-2, Информационные технологии. Методы обеспечения безопасности. Схемы цифровой подписи, обеспечивающие восстановление сообщений. Часть 2. Механизмы на основе целочисленной факторизации, 2002 г*.

Согласно ИСО/МЭК 9796 МОЖЕТ быть использована схема генерирования подписи, описанная в п. A.6, и предполагается, что это станет общепринятой практикой. Однако СЛЕДУЕТ подготовить проверочные системы для работы с МСОПД, поддерживающими активную аутентификацию подписи, генерированной как описано в п. A.4 ИСО/МЭК 9796-2.

M ДОЛЖНО состоять из M1 и M2, где M1 ДОЛЖЕН быть специальный идентификатор (Nonce) длиной c — 4 бит, а M2 является RND.IFD. Завершающий вариант 1 ДОЛЖЕН использоваться в случае SHA-1; без SHA-1 ДОЛЖЕН использоваться вариант 2.

Результатом вычисления подписи ДОЛЖНА быть подпись σ без невосстановимой части сообщения M2.

Конкретно, IFD (проверочная система) и ICC (бесконтактная МСОПД) выполняют следующие этапы:

1) IFD генерирует специальный идентификатор (Nonce) RND.IFD и посылает его на ICC, используя команду INTERNAL AUTHENTICATE.

2) ICC выполняет следующие операции:
   a) создает заголовок,
   b) генерирует M1,
   c) вычисляет h(M),
   d) создает завершитель,
   e) вычисляет репрезентативное значение сообщения F,
   f) вычисляет подпись σ и посылает ответ на IFD.

3) IFD верифицирует ответ по посланной команде INTERNAL AUTHENTICATE и проверяет, выдала ли ICC правильное значение.

ДОБАВЛЕНИЕ (НОРМАТИВНОЕ) 5 к разделу IV

БАЗОВЫЙ КОНТРОЛЬ ДОСТУПА И БЕЗОПАСНЫЙ ОБМЕН СООБЩЕНИЯМИ

A5.1 Механизм выработки ключей

Вычисление двух 3DES ключей из начального числа ключа (K_{seed}) используется как для установления базовых ключей доступа к документу (K_{ENC} и K_{MAC}), так и для установления сеансовых ключей для безопасного обмена сообщениями.

32-битный счетчик с используется для выработки нескольких ключей из одного начального числа. В зависимости от того, используется ли ключ для шифрования или для вычисления MAC ДОЛЖНЫ использоваться следующие значения:

- c = 1 (т. е. ‘0x 00 00 00 01’) для шифрования;
- c = 2 (т. е. ‘0x 00 00 00 02’) для вычисления MAC.

Для выработки двух 3DES ключей из начального числа K_{seed} и c выполняются следующие этапы:

1. Пусть D является конкатенацией K_{seed} и c ($D = K_{seed} || c$).
2. Вычислить H = SHA-1(D), SHA-1 хэш D.
3. Байты 1..8 H формируют ключ K_a, а байты 9..16 H формируют ключ K_b.
4. Скорректировать биты четности ключей K_a и K_b для формирования правильных DES ключей.

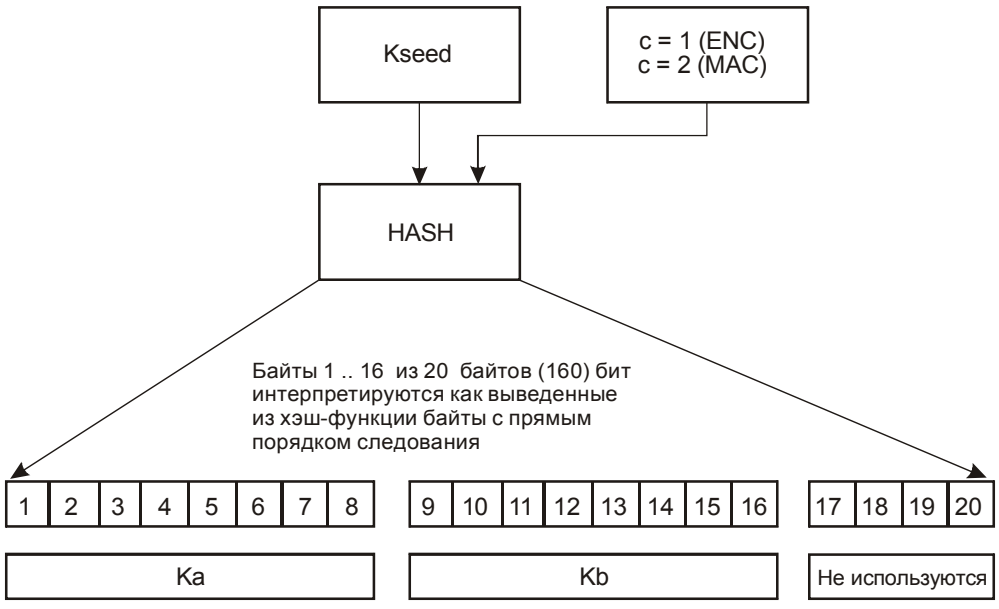


Рис. A5-1. Схема вычисления ключей из начального числа ключа

A5.2 Аутентификация и установление ключей

Аутентификация и установление ключей обеспечиваются трехпроходным запросно-ответным протоколом в соответствии с механизмом установления ключей 6 стандарта ИСО/МЭК 11770-2 с использованием 3DES как блочного шифра. Криптографическая контрольная сумма согласно МАК алгоритму 3 ИСО/МЭК 9797-1 вычисляется и добавляется к шифртекстам. Режимы работы, описываемые в п. 5.4 добавления 5, ДОЛЖНЫ использоваться. Размер специальных идентификаторов (Nonce), которыми осуществляется обмен, ДОЛЖЕН составлять 8 байтов, а обмениваемого ключевого материала –16 байтов. Отличительные идентификаторы НЕ ДОЛЖНЫ использоваться.

IFD и ICC конкретно выполняют следующие этапы:

1) IFD запрашивает RND.ICC, посылая команду GET CHALLENGE. ICC генерирует и отвечает специальным идентификатором RND.ICC.

2) IFD выполняет следующие операции:
   a) Генерирует специальный идентификатор RND.IFD и ключевой материал K.IFD.
   b) Генерирует конкатенацию S = RND.IFD || RND.ICC || K.IFD.
   c) Вычисляет криптограмму E_IFD = E[K_ENC](S).
   d) Вычисляет контрольное число M_IFD = MAC[K_MAC](E_IFD).
   e) Посылает команду MUTUAL AUTHENTICATE с использованием данных E_IFD || M_IFD.

3) ICC выполняет следующие операции:
   a) Проверяет контрольную сумму M_IFD криптограммы E_IFD.
   b) расшифровывает криптограмму E_IFD.
   c) Извлекает RND.ICC из S и проверяет, выдало ли IFD правильное значение.
   d) Генерирует ключевой материал K.ICC.
   e) Генерирует конкатенацию R = RND.ICC || RND.IFD || K.ICC
   f) Вычисляет криптограмму E_ICC = E[K_ENC](R).
   g) Вычисляет контрольное число M_ICC = MAC[K_MAC](E_ICC).
   h) Посылает ответ с использованием данных E_ICC || M_ICC.

4) IFD выполняет следующие операции:
   a) Проверяет контрольную сумму M_ICC криптограммы E_ICC.
   b) Расшифровывает криптограмму E_ICC.
   c) Извлекает RND.IFD из R и проверяет, выдало ли ICC правильное значение.

A5.3 Безопасный обмен сообщениями

После успешного выполнения протокола аутентификации IFD и ICC вычисляют сеансовые ключи KS_ENC и KS_MAC с использованием механизма установления ключей, описываемого в п. 5.1 добавления 5 с (K.ICC xor K.IFD) в качестве начального заполнения генератора ключей. Вся дальнейшая передача данных ДОЛЖНА защищаться методом безопасного обмена сообщениями в режиме MAC_ENC.

A5.3.1 *Структура сообщений SM APDU*

Объекты данных SM ДОЛЖНЫ использоваться в соответствии с таблицей A5-1 в следующем порядке:

- APDU команды: [DO‘87’] [DO‘97’] DO‘8E’.
- APDU ответа: [DO‘87’] DO‘99’ DO‘8E’.

Все объекты данных SM ДОЛЖНЫ быть закодированы в BER TLV, как указано в ИСО/МЭК 7816-4. Заголовок команды ДОЛЖЕН быть включен в вычисление в MAC, поэтому ДОЛЖЕН использоваться байт класса CLA = 0x0c.

Фактическое значение Lc будет изменено на Lc’ после применения безопасного обмена сообщениями. При необходимости соответствующий объект данных факультативно можно включать в данные APDU для передачи исходного значения Lc. В защищенном APDU команды *новый* байт *Le* ДОЛЖЕН быть ‘00’.

Таблица A5-1. Использование объектов данных SM

	DO‘85’ *	**DO‘87’ ***	**DO‘97’**	**DO‘99’**	**DO‘8E’**
Значение	Криптограм-ма (простое значение, закодиро-ванное в BER-TLV, но без объектов данных SM)	Байт индикатора заполнения содержания (‘01’ для заполнения согласно ИСО), за которым следует криптограмма	Le (защищается CC)	Processing status (SW1-SW2, protected by MAC)	Криптографич еская контрольная сумма (MAC)
APDU команды	Обязатель-ный, если данные посылаются, в противном случае отсутствуют	Обязательный, если данные посылаются, в противном случае отсутствуют	Обязательный, если данные посылаются, в противном случае отсутствуют	Не используется	Обязательный
APDU ответа	Обязатель-ный, если данные воз-вращаются, в противном случае отсутствуют	Обязательный, если данные возвращаются, в противном случае отсутствуют	Не используется	Обязательный, если данные отсутствуют, в противном случае факультативный, однако использовать рекомендуется	Обязательный

* Используется DO ‘85’ (нечетный байт INS) или DO ‘87’ (четный байт INS).

На рис. A5-2 показана схема преобразования незащищенного APDU команды в защищенный APDU команды в случае наличия *данных* и *Le*. Если *данные* отсутствуют, построение DO ‘87’ не осуществляется. Если *Le* отсутствует, построение DO ‘97’ не осуществляется. В разделе 6.4 в ИСО/МЭК 7816-4,2005 г., указывается " Нулевой и пустой объект данных Le означает максимум, т.е. . 256 или 65536 в зависимости от того, короткое или расширенное новое поле Le. Чтобы не возникало неоднозначности, РЕКОМЕНДУЕТСЯ не использовать пустое поле значения объекта данных Le.

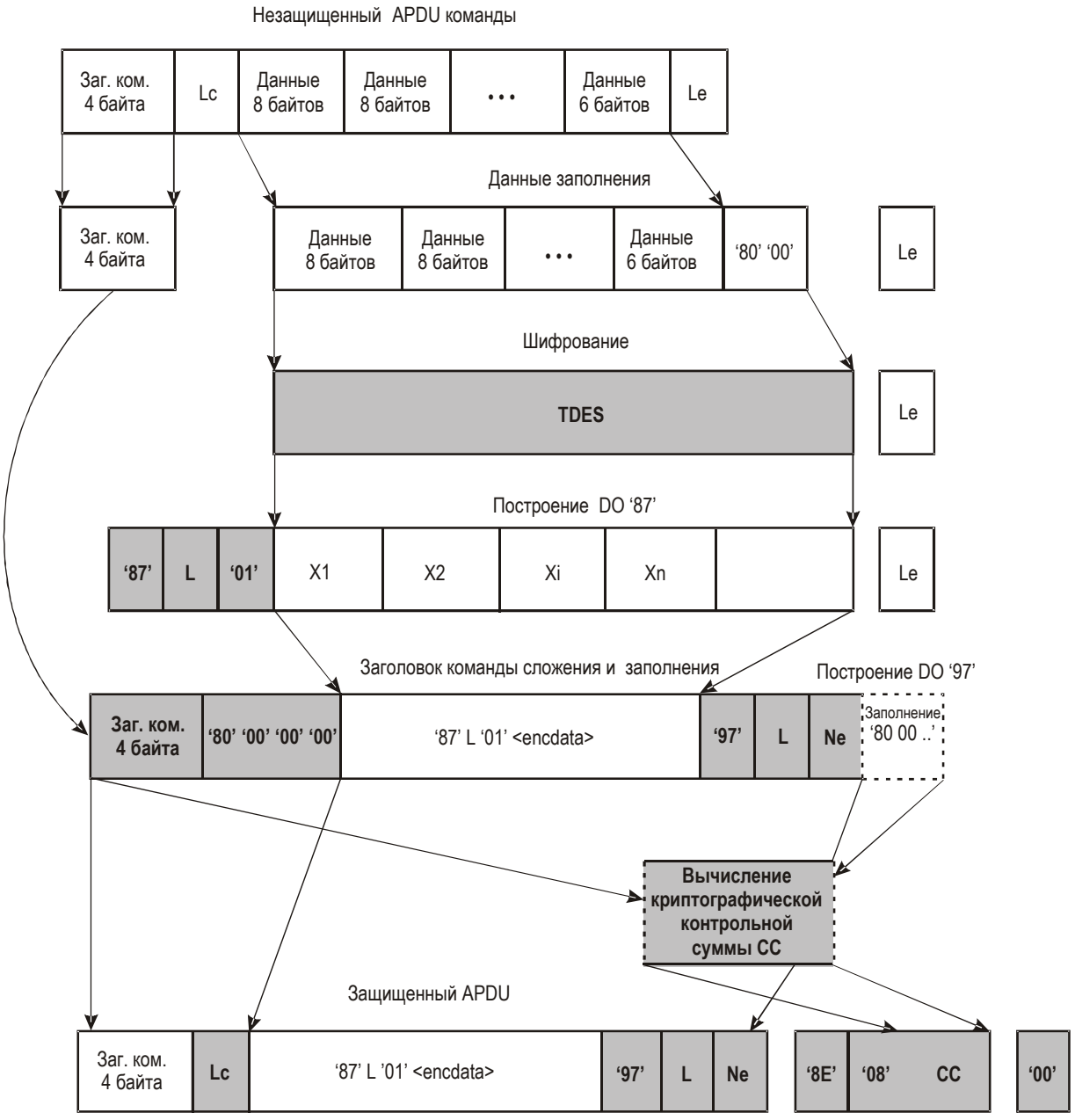


Рис. А5-2. Вычисление SM APDU команды для четного байта INS

На рис. А5-3 показана схема преобразования незащищенного APDU ответа в защищенный APDU ответа в случае наличия *данных*. Если *данные* отсутствуют, построение DO ‘87’ не осуществляется.

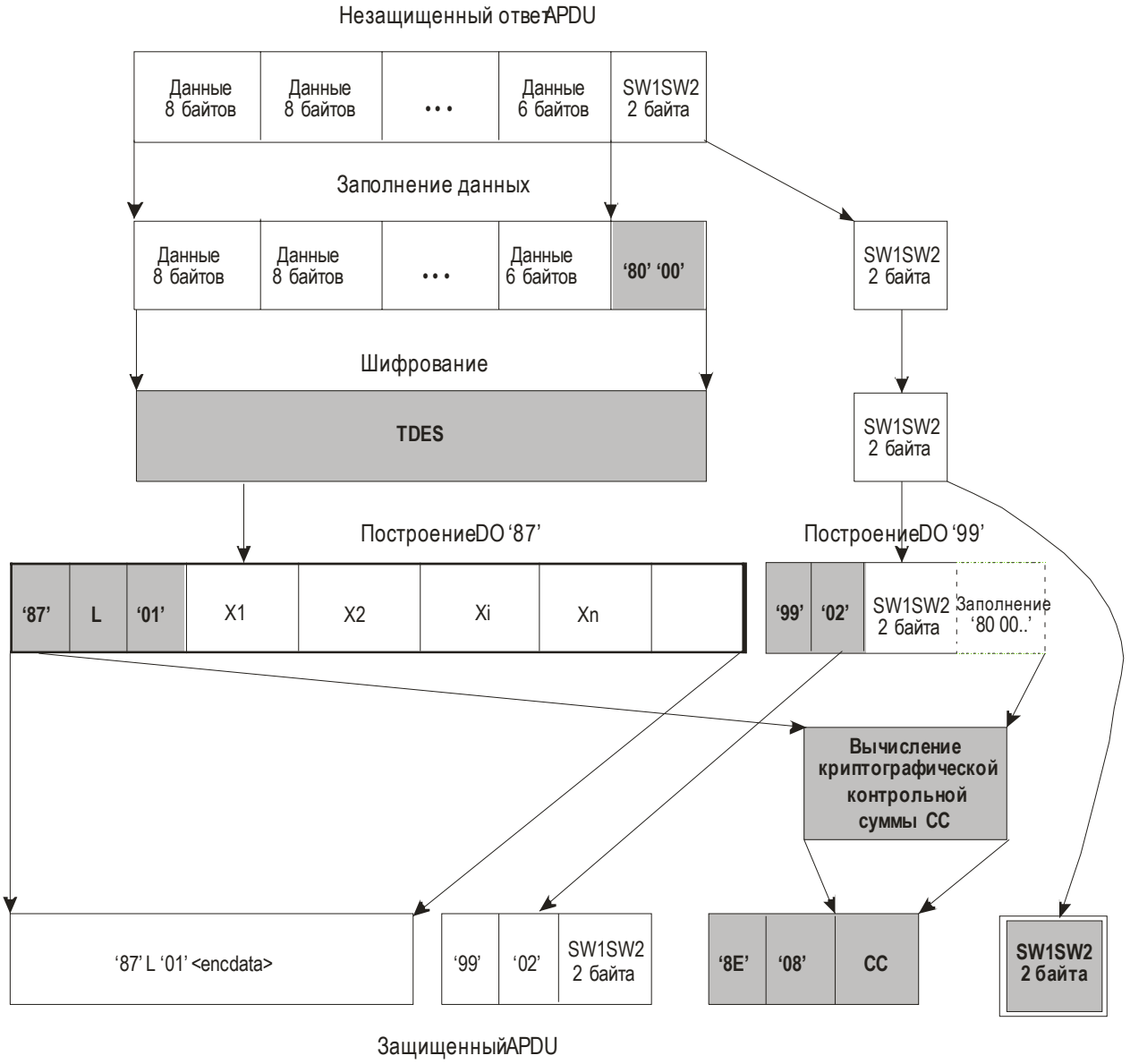


Рис. А5-3. Вычисление SM APDU ответа для четного байта INS

A5.3.2 *Ошибки SM*

Прерывание защищенного канала прикладной программы лица, подписывающего документы (LDS), имеет место в следующих случаях:

- бесконтактная ИС обесточена
- бесконтактная ИС опознает ошибку SM в процессе интерпретации команды. В этом случае байты состояния должны быть возвращены без SM. Это могут быть следующие байты состояния:

  - '6987': ожидаемые объекты данных SM отсутствуют,
  - '6988': объекты данных SM неверны.

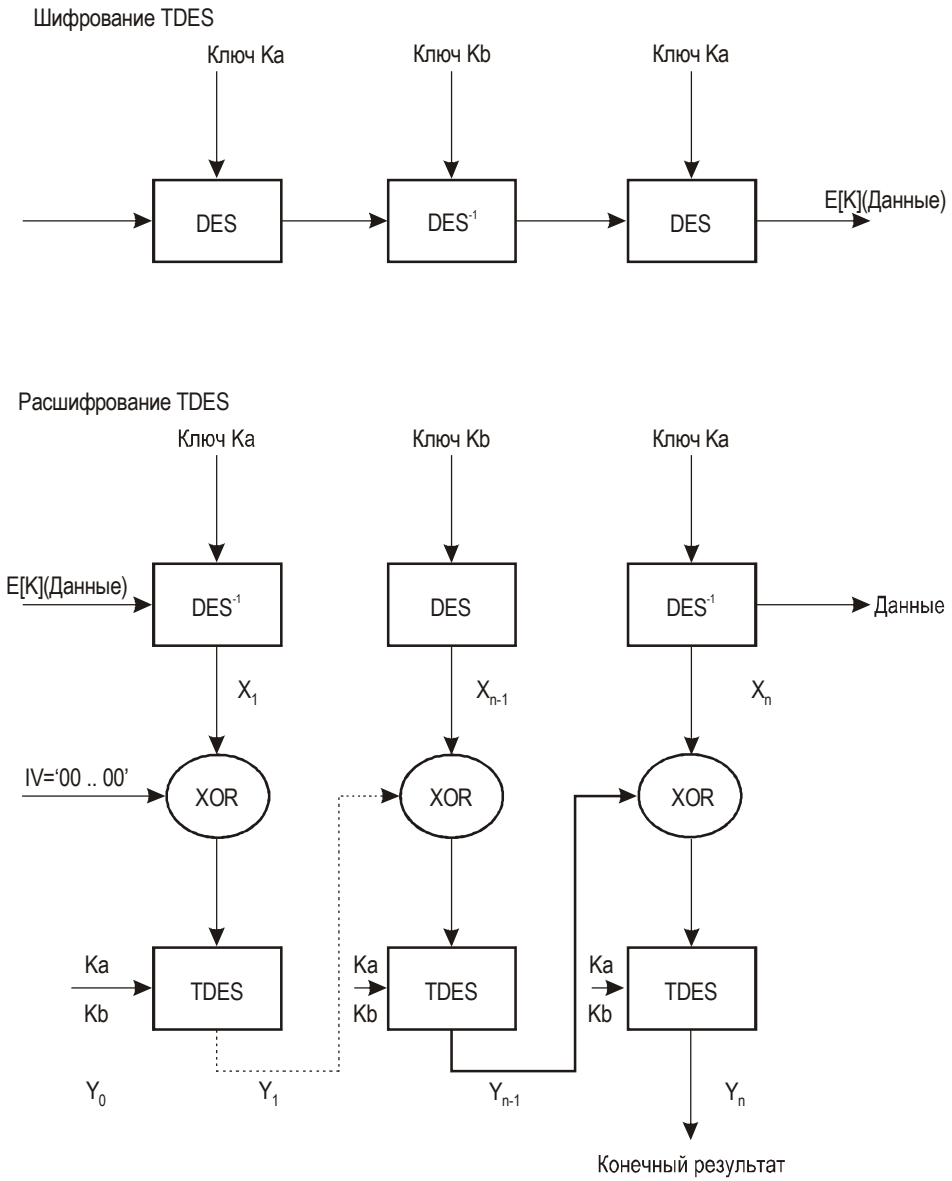
Примечание. МОГУТ быть другие обстоятельства, в которых ICC прерывает сеанс. Невозможно составить всеобъемлющий перечень таких обстоятельств.

A5.4 Режимы работы DES

В операциях DES РЕКОМЕНДУЕТСЯ использовать трехкратный DES (3DES). НЕ СЛЕДУЕТ использовать однократный DES.

A5.4.1 *Шифрование*

Используется двухключевой 3DES в режиме CBC с нулем IV (т. е. 0x00 00 00 00 00 00 00 00) в соответствии со стандартом ИСО 11568-2 (см. рис A5-4). При выполнении команды MUTUAL AUTHENTICATE заполнение для вводимых данных не используется. При вычислении SM APDU используется заполнение в соответствии с методом заполнения 2 стандарта ИСО/МЭК 9797-1.



IV – нулевая инициализация/вектор

'X_1II ... II$^{X}_{n}$' – открытый текст (сообщение подлежит шифрованию), где длина каждого блока X_1 составляет 64-бита

'Y_1II ... II$^{Y}_{n}$' – итоговая криптограмма (зашифрованное сообщение), где длина каждого блока Y_1 составляет 64-бита

Рис. A5-4. Шифрование/дешифрование 3DES в режиме CBC

A5.4.2 *Аутентификация сообщений*

Криптографические контрольные суммы вычисляются с использованием MAC алгоритма 3 стандарта ИСО/МЭК 9797-1 с блочным шифром DES (ноль IV (8 байтов)) и метода заполнения 2 стандарта ИСО/МЭК 9797-1. Длина MAC ДОЛЖНА быть 8 байтов.

После успешной аутентификации датаграмма, подлежащая кодированию с помощью MAC, ДОЛЖНА быть добавлена к началу счетчиком посылаемых команд. Счетчик посылаемых команд вычисляется путем конкатенации четырех наименее значимых байтов RND.ICC и RND.IFD соответственно:

SSC = RND.ICC (4 наименее значимых байта) || RND.IFD (4 наименее значимых байта).

Значение счетчика посылаемых команд увеличивается каждый раз перед вычислением MAC, т. е. если начальное значение составляет x, то в следующей команде значение SSC составляет x+1. Значение первого ответа тогда составляет x+2.

Для команды MUTUAL AUTHENTICATE первоначальный проверочный блок Y_0 ДОЛЖЕН быть установлен на ноль ‘0000000000000000’.

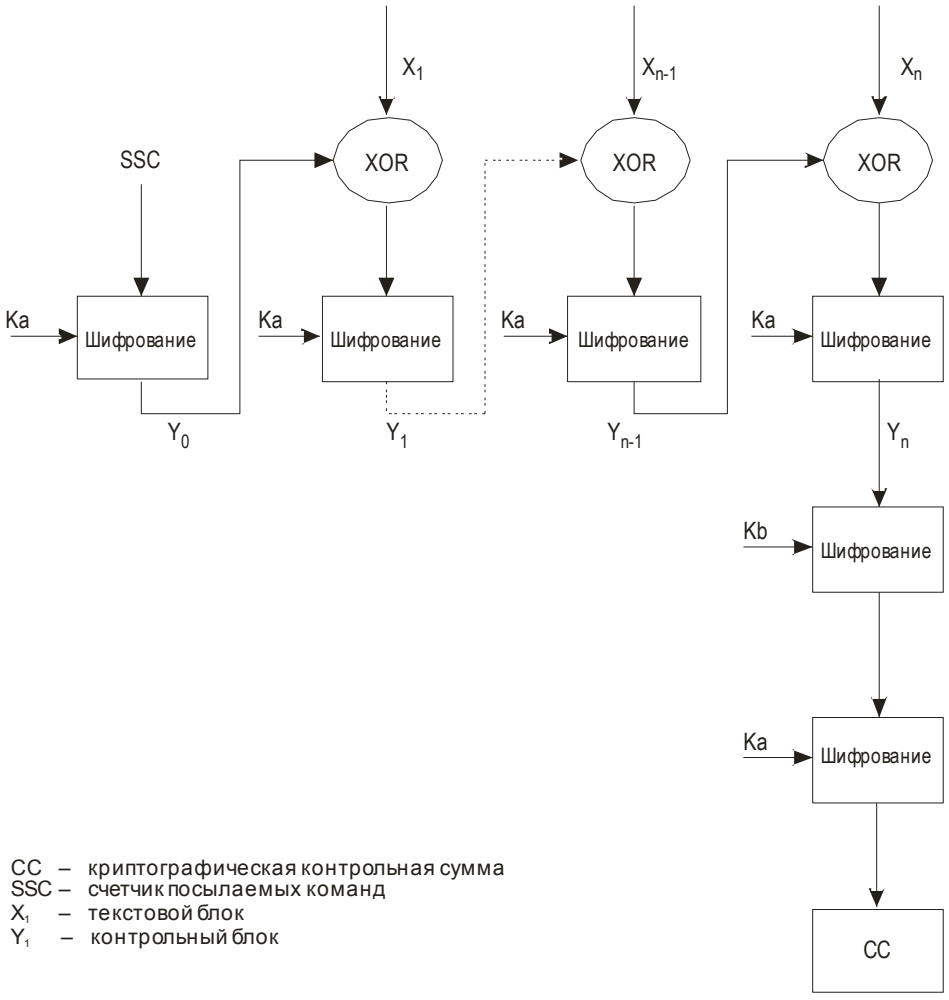


Рис. A5-5. Вычисление MAC

ДОБАВЛЕНИЕ 6 (ИНФОРМАТИВНОЕ) к разделу IV

ПРИМЕРЫ С РЕШЕНИЯМИ

A6.1 Последовательность команд

A6.1.1 *Базовый контроль доступа и безопасный обмен сообщениями на основе МСЗ*

Вычисление ключей из начального числа ключа (K_{seed})

Ввод:

K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'

Вычисление ключа шифрования (c = '00000001'):

1. Конкатенация K_{seed} и c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000001'

2. Вычисление SHA-1 хэш D:
   H_{SHA-1}(D) = 'AB94FCEDF2664EDFB9B291F85D7F77F27F2F4A9D'

3. Формирование ключей K_a и K_b:
   K_a = 'AB94FCEDF2664EDF'
   K_b = 'B9B291F85D7F77F2'

4. Корректировка битов четности:
   K_a = 'AB94FDECF2674FDF'
   K_b = 'B9B391F85D7F76F2'

Вычисление ключа расчета MAC (c = '00000002'):

1. Конкатенация K_{seed} и c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000002'

2. Вычисление SHA-1 хэш D:
   H_{SHA-1}(D) = '7862D9ECE03C1BCD4D77089DCF131442814EA70A'

3. Формирование ключей K_a и K_b:
   K_a = '7862D9ECE03C1BCD'
   K_b = '4D77089DCF131442'

4. Корректировка битов четности:
   K_a = '7962D9ECE03D1ACD'
   K_b = '4C76089DCE131543'

Получение базовых ключей доступа к документу (K_{ENC} и K_{MAC})

МСЗ ПД-2, номер документа состоит более чем из 9 знаков

1. Считывание МСЗ
   МСЗ = `I<UTOSTEVENSON<<PETER<JOHN<<<<<<<<<<`
   `D23145890<UTO3407127M95071227349<<<8`

2. Построение ‘зоны МСЗ информации’ из МСЗ
   Номер документа = `D23145890734` контрольная цифра = 9
   Дата рождения = `340712` контрольная цифра = 7
   Дата истечения срока действия = `950712` контрольная цифра = 2
   МСЗ_информация = `D231458907349340712795071 22`

Продолжить этап 3

МСЗ ПД-2, номер документа состоит из 9 знаков

1. Считывание МСЗ
   МСЗ = `I<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<`
   `L898902C<3UTO6908061F9406236<<<<<<<8`

2. Построение ‘МСЗ_информации’ из МСЗ:
   Номер документа = `L898902C<` контрольная цифра = `3`
   Дата рождения = `690806` контрольная цифра = `1`
   Дата истечения срока действия = `940623` контрольная цифра = `6`
   МСЗ_информация = `L898902C<3690806194062 36`

Продолжить этап 3

МСЗ ПД-1, номер документа состоит более чем из 9 знаков

1. Считывание МСЗ
   МСЗ = `I<UTOD23145890<7349<<<<<<<<<<`
   `3407127M9507122UTO<<<<<<<<<<2`
   `STEVENSON<<PETER<JOHN<<<<<<<<<`

2. Построение ‘зоны МСЗ информации’ из МСЗ
   Номер документа = `D23145890734` контрольная цифра = 9
   Дата рождения = `340712` контрольная цифра = 7
   Дата истечения срока действия = `950712` контрольная цифра = 2
   МСЗ_информация = `D231458907349340712795071 22`

Продолжить этап 3

МСЗ ПД-1, номер документа состоит из 9 знаков

1. Считывание МСЗ
   МСЗ = `I<UTOL898902C<3<<<<<<<<<<<<<<`
   `6908061F9406236UTO<<<<<<<<<<1`
   `ERIKSSON<<ANNA<MARIA<<<<<<<<<<`

2. Построение ‘МСЗ_информации’ из МСЗ:
   Номер документа = `L898902C<` контрольная цифра = `3`
   Дата рождения = `690806` контрольная цифра = `1`
   Дата истечения срока действия = `940623` контрольная цифра = `6`
   МСЗ_информация = `L898902C<3690806194062 36`

3. Вычисление SHA-1 хэш 'МСЗ_информации':
H_{SHA-1}(МСЗ_информация) = '239AB9CB282DAF66231DC5A4DF6BFBAEDF477565'

4. Использование наиболее значимых 16 байтов для формирования K_{seed}:
K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'

5. Вычисление базовых ключей доступа (K_{ENC} и K_{MAC}) согласно п. А5.1 добавления 5:
K_{ENC} = 'AB94FDECF2674FDFB9B391F85D7F76F2'
K_{MAC} = '7962D9ECE03D1ACD4C76089DCE131543'

Аутентификация и установление сеансовых ключей

Проверочная система:

1. Запрос 8-байтового произвольного числа с бесконтактной ИС МСОПД:

APDU команды:

CLA	INS	P1	P2	LE
00h	84h	00h	00h	08h

APDU ответа:

Поле данных ответа	SW1SW2
RND.ICC	9000h

RND.ICC = '4608F91988702212'

2. Генерирование 8-байтового и 16-байтового произвольного числа:
RND.IFD = '781723860C06C226'
K_{IFD} = '0B795240CB7049B01C19B33E32804F0B'

3. Конкатенация RND.IFD, RND.ICC и K_{IFD}:
S = '781723860C06C2264608F91988702212
0B795240CB7049B01C19B33E32804F0B'

4. Шифрование S с ключом TDES K_{ENC}, как вычислено в п. А5.2 добавления 5:
E_{IFD} = '72C29C2371CC9BDB65B779B8E8D37B29
ECC154AA56A8799FAE2F498F76ED92F2'

5. Вычисление MAC по E_{IFD} с ключом TDES K_{MAC}, как вычислено в п. А5.2 добавления 5:
M_{IFD} = '5F1448EEA8AD90A7'

6. Построение данных команды MUTUAL AUTHENTICATE и посылка APDU команды на бесконтактную ИС МСОПД:
cmd_data = '72C29C2371CC9BDB65B779B8E8D37B29ECC154AA
56A8799FAE2F498F76ED92F25F1448EEA8AD90A7'

APDU команды:

CLA	INS	P1	P2	LC	Поле данных команды	LE
00h	82h	00h	00h	28h	cmd_data	28h

Бесконтактная ИС МСОПД:

1. Дешифрование и верификация полученных данных и сравнение RND.ICC с ответом на команду GET CHALLENGE.

2. Генерирование 16-байтового произвольного числа:
K_{ICC} = `'0B4F80323EB3191CB04970CB4052790B'`

3. Вычисление XOR K_{IFD} и K_{ICC}:
K_{seed} = `'0036D272F5C350ACAC50C3F572D23600'`

4. Вычисление сеансовых ключей (KS_{ENC} и KS_{MAC}) с использованием п. A5.1 добавления 5:
KS_{ENC} = `'979EC13B1CBFE9DCD01AB0FED307EAE5'`
KS_{MAC} = `'F1CB1F1FB5ADF208806B89DC579DC1F8'`

5. Вычисление счетчика посылаемых команд:
SSC = `'887022120C06C226'`

6. Конкатенация RND.ICC, RND.IFD и K_{ICC}:
R = `'4608F91988702212781723860C06C226`
`0B4F80323EB3191CB04970CB4052790B'`

7. Шифрование R с ключом TDES K_{ENC}, как вычислено в п. A5.2 добавления 5:
E_{ICC} = `'46B9342A41396CD7386BF5803104D7CE`
`DC122B9132139BAF2EEDC94EE178534F'`

8. Вычисление MAC по E_{ICC} с ключом TDES K_{MAC}, как вычислено в п. A5.2 добавления 5:
M_{ICC} = `'2F2D235D074D7449'`

9. Построение данных ответа на команду MUTUAL AUTHENTICATE и посылка APDU ответа в проверочную систему:

resp_data = `'46B9342A41396CD7386BF5803104D7CEDC122B91`
`32139BAF2EEDC94EE178534F2F2D235D074D7449'`

APDU ответа:

Поле данных ответа	SW1SW2
resp_data	9000h

Проверочная система:

1. Дешифрование и верификация полученных данных и сравнение полученного RND.IFD с генерированным RND.IFD.

2. Вычисление XOR K_{IFD} и K_{ICC}:
   K_{seed} = '0036D272F5C350ACAC50C3F572D23600'

3. Вычисление сеансовых ключей (KS_{ENC} и KS_{MAC}) с использованием п. A5.1 добавления 5:
   KS_{ENC} = '979EC13B1CBFE9DCD01AB0FED307EAE5'
   KS_{MAC} = 'F1CB1F1FB5ADF208806B89DC579DC1F8'

4. Вычисление счетчика посылаемых команд:
   SSC = '887022120C06C226'

Безопасный обмен сообщениями

После аутентификации и установления сеансовых ключей система проверки выбирает EF.COM (файл ID = '011E') и считывает данные, используя метод безопасного обмена сообщениями. Будут использоваться вычисленные KS_{ENC}, KS_{MAC} и SSC (предыдущие этапы 18 и 19).

Сначала выбирается EF.COM, затем первые четыре байта этого файла считываются для определения длины структуры файла, после чего считываются остальные байты.

1. Выбор EF.COM

   Незащищенный APDU команды:

CLA	INS	P1	P2	LC	Поле данных команды
00h	A4h	02h	0Ch	02h	01h 1Eh

   a. Маскирование байта класса и заполнение заголовка команды:
      Заголовок команды = '0CA4020C80000000'

   b. Данные заполнения:
      Данные = '011E800000000000'

   c. Шифрование данных с KS_{ENC}:
      Зашифрованные данные = '6375432908C044F6'

   d. Построение DO'87':
      DO87 = '8709016375432908C044F6'

   e. Конкатенация заголовка команды и DO87:
      M = '0CA4020C8000000087090163754329 08C044F6'

   f. Вычисление MAC от M:
      i. приращение SSC на 1:
         SSC = '887022120C06C227'
      ii. конкатенация SSC и M и добавление заполнения:
         N = '887022120C06C2270CA4020C80000000
         8709016375432908C044F68000000000'
      iii. Вычисление MAC по N с KS_{MAC}:
      CC = 'BF8B92D635FF24F8'

   g. Построение DO'8E':
      DO8E = '8E08BF8B92D635FF24F8'

h. Построение и посылка защищенного APDU:
Защищенный APDU = ‘0CA4020C158709016375432908C0
44F68E08BF8B92D635FF24F800’

i. Получение APDU ответа бесконтактной ИС МСОПД:
RAPDU = ‘990290008E08FA855A5D4C50A8ED9000’

j. Верификация RAPDU CC путем вычисления MAC DO’99’:
i. Приращение SSC на 1:
SSC = ‘887022120C06C228’
ii. Конкатенация SSC и DO‘99’ и добавление заполнения:
K = ‘887022120C06C2289902900080000000’
iii. Вычисление MAC с KS_{MAC}:
CC’ = ‘FA855A5D4C50A8ED’
iv. Сравнение CC’ с данными DO‘8E’ RAPDU.
‘FA855A5D4C50A8ED’ == ‘FA855A5D4C50A8ED’ ? ДА.

2. Считывание двоичного файла первых четырех байтов:

Незащищенный APDU команды:

CLA	INS	P1	P2	LE
00h	B0h	00h	00h	04h

a. Маскирование байта класса и заполнение заголовка команды:
Заголовок команды = ‘0CB0000080000000’

b. Построение DO‘97’:
DO97 = ‘970104’

c. Конкатенация заголовка команды и DO97:
M = ‘0CB0000080000000970104’

d. Вычисление MAC от M:
i. Приращение SSC на 1:
SSC = ‘887022120C06C229’
ii. Конкатенация SSC и M и добавление заполнения:
N = ‘887022120C06C2290CB00000
8000000097010480000000000’
iii. Вычисление MAC по N с KS_{MAC}:
CC = ‘ED6705417E96BA55’

e. Построение DO‘8E’:
DO8E = ‘8E08ED6705417E96BA55’

f. Построение и посылка защищенного APDU:
Защищенный APDU = ‘0CB000000D9701048E08ED6705417E96BA5500’

g. Получение APDU ответа бесконтактной ИС МСОПД:
RAPDU = ‘8709019FF0EC34F992265199029000
8E08AD55CC17140B2DED9000’

h. Верификация RAPDU CC путем вычисления MAC конкатенации DO‘87’ и DO‘99’:
   i. Приращение SSC на 1:
      SSC = ‘887022120C06C22A’
   ii. Конкатенация SSC, DO‘87’ и DO‘99’ и добавление заполнения:
      K = ‘887022120C06C22A8709019F
      F0EC34F99226519902900080’
   iii. Вычисление MAC с KS_{MAC}:
      CC’ = ‘AD55CC17140B2DED’
   iv. Сравнение CC’ с данными DO‘8E’ RAPDU:
      ‘AD55CC17140B2DED’ == ‘AD55CC17140B2DED’? ДА.

i. Дешифрование данных DO‘87’ с KS_{ENC}:
   Дешифрованные данные = ‘60145F01’

j. Определение длины структуры:
   L = ‘14’ + 2 = 22 байта.

3. Считывание бинарно остальных 18 байтов от смещения 4:

Незащищенный APDU команды:

CLA	INS	P1	P2	LE
00h	B0h	00h	04h	12h

a. Маскирование байта класса и заполнение заголовка команды:
   Заголовок команды = ‘0CB0000480000000’

b. Построение DO‘97’:
   DO97 = ‘970112’

c. Конкатенация заголовка команды и DO97:
   M = ‘0CB0000480000000970112’

d. Вычисление MAC от M:
   i. Приращение SSC на 1:
      SSC = ‘887022120C06C22B’
   ii. Конкатенация SSC и M и добавление заполнения:
      N = ‘887022120C06C22B0CB00004
      8000000097011280000000000’
   iii. Вычисление MAC по N с KS_{MAC}:
      CC = ‘2EA28A70F3C7B535’

e. Построение DO‘8E’:
   DO8E = ‘8E082EA28A70F3C7B535’

f. Построение и посылка защищенного APDU:
   Защищенный APDU = ‘0CB000040D9701128E082EA28A70F3C7B53500’

g. Получение APDU ответа бесконтактной ИС МСОПД:
   RAPDU = ‘871901FB9235F4E4037F2327DCC8964F1F9B8C30F42
   C8E2FFF224A990290008E08C8B2787EAEA07D749000’

h. Верификация RAPDU CC путем вычисления MAC конкатенации DO‘87’ и DO‘99’:
   i. Приращение SSC на 1:
      SSC = ‘887022120C06C22C’
   ii. Конкатенация SSC, DO‘87’ и DO‘99’ и добавление заполнения:
      K = ‘887022120C06C22C871901FB9235F4E4037F232
      7DCC8964F1F9B8C30F42C8E2FFF224A99029000’
   iii. Вычисление MAC по KS_{MAC}:
      CC’ = ‘C8B2787EAEA07D74’
   i.v Сравнение CC’ с данными DO‘8E’ RAPDU:
      ‘C8B2787EAEA07D74’ == ‘C8B2787EAEA07D74’ ? YES.

i. Расшифровка данных DO‘87’ с KS_{ENC}:
   Расшифрованные данные = ‘04303130365F36063034303030305C026175’

РЕЗУЛЬТАТ:
данные EF.COM = ‘60145F0104303130365F36063034303030305C026175’

A6.1.2 *Пассивная аутентификация*

Этап 1: считывание объекта защиты документа (SO_D) (факультативно содержит сертификат лица, подписывающего документы (C_{DS})) с бесконтактной ИС.
Этап 2: считывание данных лица, подписывающего документы (DS), с объекта защиты документа (SO_D).
Этап 3: верификация SO_D системой проверки путем использования открытого ключа лица, подписывающего документы (KPu_{DS}).
Этап 4: верификация C_{DS} системой проверки путем использования открытого ключа подписывающегося CA страны (KPu_{CSCA}).

Если обе верификации на этапе 3 и 4 правильные, то это означает, что содержанию SO_D можно доверять и его СЛЕДУЕТ использовать в процессе проверки.

Этап 5: считывание соответствующих групп данных с LDS.
Этап 6: вычисление хэш-значений соответствующих групп данных.
Этап 7: сравнение вычисленных хэш-значений соответствующими хэш-значениями в SO_D.

Если хэш-значения на этапе 7 идентичны, это означает, что содержание группы данных является аутентичным и не изменено.

A6.1.3 *Активная аутентификация*

В этом примере используются следующие установочные параметры:

1. Механизм, основанный на целостной факторизации: RSA

2. Длина модуля: 1024 бит (128 байтов)

3. Алгоритм хэширования: SHA1

Проверочная система:

Этап 1. Генерирование 8-байтового произвольного числа:
RND.IFD = ‘F173589974BF40C6’

Этап 2. Построение команды внутренней аутентификации и посылка APDU команды на бесконтактную ИС МСОПД:

APDU команды

CLA	INS	P1	P2	LC	Поле данных команды	LE
0xh	88h	00h	00h	08h	RND.IFD	00h

Бесконтактная ИС МСОПД:

Этап 3. Определение M_2 из входящего APDU:
M_2 = ‘F173589974BF40C6’

Этап 4. Создание завершителя:
T = ‘BC’ (i.e. SHA1)

Этап 5. Определение длины:
a. $c = k – L_h – 8t – 4 = 1024 – 160 – 8 – 4 = 852$ бит
b. $L_{M1} = c – 4 = 848$ бит

Этап 6. Генерирование специального идентификатора (Nonce) M_1 длиной L_{M1}:
M_1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8’

Этап 7. Создание M:
$M = M_1 | M_2$ = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6’

Этап 8. Вычисление SHA1 краткой формы M:
H = SHA1(M) = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’

Этап 9.[2] Построение репрезентатива сообщения:

F = ‘6A’ | M_1 | H | T =

‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
4E7292E2DCDA3024B47DA8C063AA1E6D
22FBD976AB0FE73D94D2D9C6D88127BC’

Этап 10. Шифрование F с помощью открытого ключа активной аутентификации для формирования подписи:

S = ‘756B683B036A6368F4A2EB29EA700F96
E26100AFC0809F60A91733BA29CAB362
8CB1A017190A85DADE83F0B977BB513F
C9C672E5C93EFEBBE250FE1B722C7CEE
F35D26FC8F19219C92D362758FA8CB0F
F68CEF320A8753913ED25F69F7CEE772
6923B2C43437800BBC9BC028C49806CF
2E47D16AE2B2CC1678F2A4456EF98FC9’

Этап 11. Построение данных ответа на команду INTERNAL AUTHENTICATE и посылка APDU ответа в систему проверки:

APDU ответа:

Поле данных ответа	**SW1SW2**
S	9000h

Система проверки:

Этап 12. Дешифровка подписи с помощью открытого ключа:

F = ‘6A9D2784A67F8E7C659973EA1AEA25D9
5B6C8F91E5002F369F0FBDCE8A3CEC19
91B543F1696546C5524CF23A5303CD6C
98599F40B79F377B5F3A1406B3B4D8F9
6784D23AA88DB7E1032A405E69325FA9
1A6E86F5C71AEA978264C4A207446DAD
4E7292E2DCDA3024B47DA8C063AA1E6D
22FBD976AB0FE73D94D2D9C6D88127BC’

Этап 13. Определение хэш-алгоритма по завершителю T*:

T = ‘BC’ (i.e. SHA1).

Этап 14. Выделение краткой формы:

D = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’

2. Поскольку известная часть (RND.IFD) не возвращена, но должна быть добавлена самим IFD, то применяется частичное восстановление (‘6A’).

Этап 15. Выделение M_1:

M1 = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8’

Этап 16. Заголовок указывает частичное восстановление, но подпись имеет длину модуля для конкатенации M_1 с известным M_2 (т. е. RND.IFD):

M* = ‘9D2784A67F8E7C659973EA1AEA25D95B
6C8F91E5002F369F0FBDCE8A3CEC1991
B543F1696546C5524CF23A5303CD6C98
599F40B79F377B5F3A1406B3B4D8F967
84D23AA88DB7E1032A405E69325FA91A
6E86F5C71AEA978264C4A207446DAD4E
7292E2DCDA3024B47DA8F173589974BF
40C6’

Этап 17. Вычисление SHA1 краткой формы M*:

D* = ‘C063AA1E6D22FBD976AB0FE73D94D2D9
C6D88127’

Этап 18. Сравнение D и D*:

D равняется D*, т. е. верификация прошла успешно.

A6.2 Срок службы

Нижеуказанные примеры поясняют, как следует вычислять срок службы ключей, описываемый в разделе 9.

A6.2.1 *Пример 1*

Первый пример демонстрирует систему, при которой государство желает, чтобы общий срок службы всех его сертификатов оставался минимальным. МСОПД государства действительны в течение пяти лет, и поскольку государство ежегодно выдает относительно большое количество МСОПД, оно решает, что периоды выдачи ключей должны быть минимальными.

Период	Истекшее время	
Выдача ключа лица, подписывающего документы		1 мес
Срок действия МСОПД	5 лет	—
Срок действия сертификата лица, подписывающего документы	5 лет	1 мес
Выдача ключа подписывающегося СА страны	3 года	—
Срок действия сертификата подписывающегося СА страны	8 лет	1 мес

Последствиями этого варианта является то, что ко времени истечения срока действия первого сертификата подписывающегося СА страны будет выдано по крайней мере 36 ключей подписи документов (один на каждый период в 1 мес) и в течение нескольких последних месяцев действия этого ключа подписывающегося СА страны по крайней мере два других ключа подписи страны будут действительны для верификации подписей.

A6.2.2 *Пример 2*

Второй пример иллюстрирует систему, при которой государство применяет менее жесткий подход. МСОПД действительны в течение 10 лет; государство решает сохранять средние периоды выдачи для всех ключей.

Период	Истекшее время	
Выдача ключа лица, подписывающего документы		2 мес
Срок действия МСОПД	10 лет	—
Срок действия сертификата лица, подписывающего документы	10 лет	2 мес
Выдача ключа подписывающегося СА страны	4 года	—
Срок действия сертификата подписывающегося СА страны	14 лет	2 мес

Последствиями этого варианта является то, что ко времени истечения срока действия первого сертификата подписывающегося СА страны будет выдано по крайней мере 24 ключа лица, подписывающего документы, и в течение нескольких последних месяцев действия ключа подписывающегося СА страны по крайней мере три других ключа подписывающегося СА страны будут действительны для верификации подписей.

A6.2.3 *Пример 3*

Последний пример иллюстрирует систему, при которой государство решает использовать максимальные пределы, рекомендуемые данной структурой. МСОПД действительны в течение десяти лет; ключ подписывающегося СА страны заменяется каждые пять лет, а ключи лица, подписывающего документы, заменяются каждые три месяца.

Период	Истекшее время	
Выдача ключа лица, подписывающего документы		3 мес
Срок действия МСОПД	10 лет	—
Срок действия сертификата лица, подписывающего документы	10 лет	3 мес
Выдача ключа подписывающегося СА страны	5 лет	—
Срок действия сертификата подписывающегося СА страны	15 лет	3 мес

Последствиями этого варианта является то, что ко времени истечения срока действия первого сертификата подписывающегося СА страны будет выдано по крайней мере 20 ключей лица, подписывающего документы, и в течение нескольких последних месяцев действия ключа подписывающегося СА страны по крайней мере три других ключа подписывающегося СА страны, будут действительны для верификации подписей.

ДОБАВЛЕНИЕ 7 (ИНФОРМАТИВНОЕ) к разделу IV

PKI И УГРОЗЫ НАРУШЕНИЯ БЕЗОПАСНОСТИ

A7.1 Управление ключами

A7.1.1 *Ключи подписывающегося CA страны и лиц, подписывающих документы*

В целях защиты закрытых ключей РЕКОМЕНДУЕТСЯ использовать для генерации подписей защищенное аппаратное оборудование (защищенное устройство создания подписей SSCD); SSCD генерирует новые пары ключей, надежно хранит и уничтожает (после истечения срока действия) соответствующий закрытый ключ. Для защиты от атак на SSCD, в том числе от атак через побочные каналы (например, тайминг, энергопотребление, электромагнитные излучения, внесение неисправностей) и атак на генераторы случайных чисел, РЕКОМЕНДУЕТСЯ использовать SSCD сертифицированные/проверенные сертифицирующим органом, отвечающим требованиям CCRA, в соответствии с надлежащим профилем общих критериев защиты с уровнем EAL 4+ SOF-High.

При распределении самоподписывающихся сертификатов CA страны по дипломатическим каналам необходимо проявлять крайнюю осторожность для предотвращения внесения жульнического сертификата подписывающегося CA страны. Кроме того, РЕКОМЕНДУЕТСЯ, чтобы государства надежно хранили полученные сертификаты подписывающегося CA страны и чтобы доступ к ним предоставлялся считывающим устройствам безопасным образом. Для защиты от атак на CAD, РЕКОМЕНДУЕТСЯ использовать CAD, сертифицированные/проверенные сертифицирующим органом, отвечающим требованиям CCRA, в соответствии с надлежащим профилем общих критериев защиты с уровнем EAL 4+ SOF-High.

A7.1.2 *Ключи активной аутентификации*

Пары ключей активной аутентификации РЕКОМЕНДУЕТСЯ генерировать безопасным способом. Поскольку закрытый ключ хранится на бесконтактной ИС в защищенной памяти, а конструкция бесконтактной ИС должна противостоять атакам на протяжении всего срока действия МСОПД, РЕКОМЕНДУЕТСЯ использовать бесконтактные ИС, сертифицированные/проверенные сертифицирующим органом, отвечающим требованиям CCRA, в соответствии с надлежащим профилем общих критериев защиты с уровнем EAL 4+ SOF-High.

Существующая технология бесконтактных ИС влияет на максимальную длину ключей, используемых внутри бесконтактной ИС для активной аутентификации. Многие бесконтактные ИС в настоящее время не поддерживают длину ключей, превышающую безопасный уровень в 80 бит, что является причиной выбора этого значения в качестве рекомендуемого минимума. Это относительно невысокий уровень безопасности с учетом срока действия МСОПД. В этой связи РЕКОМЕНДУЕТСЯ использовать более длинные ключи, если они поддерживаются бесконтактной ИС.

Государствам, использующим механизм активной аутентификации для подтверждения подлинности иностранного МСОПД, следует также иметь в виду, что механизм отзыва скомпрометированных ключей активной аутентификации не установлен.

A7.1.3 *Атаки, вызывающие отказ в обслуживании*

При использовании государствами директории для распределения сертификатов лиц, подписывающих документы, и CRL необходимо учитывать возможность отказа в обслуживании в результате атаки. Такие атаки предотвратить невозможно. В этой связи РЕКОМЕНДУЕТСЯ, чтобы сертификат лица, подписывающего документы, требующийся для валидации объекта защиты документа, включался также в сам объект защиты. Принимающим государствам СЛЕДУЕТ использовать предоставленный сертификат лица, подписывающего документы.

Для двустороннего распределения CRL РЕКОМЕНДУЕТСЯ устанавливать несколько каналов (например, Интернет, телефон, факсимильная связь, почта и т. д.) с другими государствами и подтверждать получение поступивших CRL.

A7.2 Угрозы дублирования

Копирование подписанных данных, хранящихся на бесконтактной ИС, произвести вполне возможно. Государствам, обеспокоенным возможностью перекопирования данных своих граждан на другую бесконтактную ИС, следует осуществлять активную аутентификацию, чтобы обеспечить обнаружение таких попыток.

A7.2.1 *Пассивная аутентификация*

Пассивная аутентификация не предотвращает копирования данных, хранящихся на бесконтактной ИС. Следовательно, бесконтактная ИС МСОПД может быть заменена поддельной бесконтактной ИС, хранящей данные, скопированные с бесконтактной ИС другого МСОПД. Принимающим государствам СЛЕДУЕТ убеждаться в том, что считанные с бесконтактной ИС данные действительно принадлежат предъявленному МСОПД. Это может делаться путем сравнения DG1, хранящейся на бесконтактной ИС, с MRZ, напечатанной на МСОПД. Если DG1 и MRZ сопоставимы, объект защиты документа действителен, а предъявленный МСОПД не фальшивый (не подделан), то можно считать, что МСОПД и хранящиеся на бесконтактной ИС данные принадлежат друг другу.

A7.2.2 *Активная аутентификация*

Активная аутентификация усложняет подмену бесконтактной ИС, но не делает ее невозможной. МСОПД, предъявленный злоумышленником проверочной системе, может быть оснащен специальной бесконтактной ИС. Эта бесконтактная ИС действует в качестве заменителя подлинной бесконтактной ИС, находящейся на удалении; бесконтактная ИС взаимодействует со злоумышленником, злоумышленник взаимодействует с другим злоумышленником, и этот другой злоумышленник получает доступ (временно) к подлинной бесконтактной ИС. Проверочная система не способна заметить, что она аутентифицирует не предъявленную бесконтактную ИС, а бесконтактную ИС, находящуюся на некотором расстоянии. Такое нападение называется гроссмейстерской атакой.

A7.3 Угрозы нарушения конфиденциальности

A7.3.1 *Отсутствие контроля доступа*

Использование бесконтактных ИС, действующих через малый зазор, уже свело к минимуму риски нарушения конфиденциальности, так как считывающие устройства должны находиться на

очень близком расстоянии от бесконтактной ИС и поэтому скимминг уже не является серьезной угрозой. Однако перехват передач данных между бесконтактной ИС и считывателем возможен с большего расстояния. Государствам, желающим устранить эту угрозу, СЛЕДУЕТ осуществлять базовый контроль доступа.

A7.3.2 *Базовые ключи доступа*

Базовые ключи доступа, используемые для аутентификации считывателя и настройки сеансовых ключей для шифрования передач данных между бесконтактной ИС и считывателем, генерируются из состоящего из 9 цифр номера документа, даты рождения и даты истечения срока действия. Таким образом, энтропия ключей является относительно низкой. У МСОПД со сроком действия десять лет энтропия составляет максимум 56 бит. При наличии дополнительных сведений (например, приблизительный возраст держателя или связь между номером документа и датой истечения срока действия) энтропия снижается еще больше. Вследствие относительно низкой энтропии, злоумышленник в принципе может записать зашифрованный сеанс, вычислить грубым методом базовые ключи доступа на основе аутентификации, вывести сеансовые ключи и расшифровать записанный сеанс. Однако это все-таки требует значительных усилий по сравнению с получением данных из других источников.

A7.3.3 *Активная аутентификация (трассировка данных)*

В запросно-ответном протоколе, используемом для активной аутентификации, бесконтактная ИС помечает битовую строку, выбранную более или менее произвольно проверочной системой. Если принимающее государство использует текущую дату, время и местонахождение для генерации этой битовой строки непредсказуемым, но поддающимся проверке способом (например, с использованием защищенного аппаратного оборудования), третья сторона впоследствии может быть уверена в том, что подписывающее документ лицо находилось в определенный день и время в определенном месте.

A7.4 Криптографические угрозы

Рекомендуемая минимальная длина ключей выбрана с таким расчетом, чтобы для расшифрования этих ключей необходимо было приложить определенные (как предполагается) усилия вне зависимости от выбранного алгоритма подписи.

Тип ключа	Уровень защиты
Подписывающийся CA страны	128 бит
Лицо, подписывающее документы	112 бит
Активная аутентификация	80 бит

A7.4.1 *Прогресс математики и нестандартное вычисление*

В соответствии с законом Мура вычислительные возможности удваиваются каждые 18 месяцев. Однако защита алгоритма подписи зависит не только от вычислительных возможностей; достижения в области математики (криптоанализ) и наличие новых нестандартных методов вычисления (например, квантовые компьютеры) также необходимо учитывать.

В связи с продолжительным сроком действия ключей весьма сложно делать предсказания относительно математического прогресса и наличия нестандартных вычислительных устройств. Поэтому рекомендации в отношении длины ключей базируются главным образом на экстрапалированных вычислительных возможностях. По вышеупомянутым причинам государствам СЛЕДУЕТ часто пересматривать длину ключей для своих собственных, а также для получаемых МСОПД.

Генерирование пар ключей специальной формы может в целом повысить эффективность алгоритма подписи, и может также в будущем использоваться для криптоанализа. Тем не менее СЛЕДУЕТ избегать применения таких специальных пар ключей.

A7.4.2 *Коллизия хэш-функции*

Хотя обнаружение другого сообщения, выдающего такое же хэш-значение, как и данное сообщение в вычислительном отношении представляется нереальным, обнаружить два сообщения, выдающих одинаковые хэш-значения, значительно легче. Это называется парадоксом дня рождения.

В целом, все подписываемые сообщения производятся самим лицом, подписывающим документы. Поэтому обнаружение хэш-коллизии не может значительно помочь злоумышленнику. Однако если фотографии, представленные просителем в цифровой форме, принимаются лицом, подписывающим документы, без дополнительной рандомнизированной модификации, может иметь место следующая атака.

- Два лица совместно используют свои цифровые фотографии. Они многократно "жонглируют" небольшим числом бит в каждой фотографии до тех пор, пока две фотографии не произведут одно и то же хэш-значение.

- Оба лица просят выдать новый МСОПД, используя подделанную фотографию. Каждое лицо может теперь использовать МСОПД другого лица, при том условии, что цифровую фотографию на бесконтактной ИС можно заменить (например, путем подмены чипа).

Хэш-функция SHA-1 обеспечивает только 80 бит защиты от хэш-коллизии. Таким образом, обнаружить хэш-коллизию значительно легче, чем расшифровать ключ лица, подписывающего документы, который обеспечивает 112 бит защиты. В этой связи, если проблема хэш-коллизии вызывает озабоченность (например, как описано выше), РЕКОМЕНДУЕТСЯ не использовать SHA-1 в качестве хэш-функции.

ДОБАВЛЕНИЕ 8 (ИНФОРМАТИВНОЕ) к разделу IV

МЕХАНИЗМ РАСПРЕДЕЛЕНИЯ C_{CSCA}

A8.1 В процессе распределения самоподписывающихся сертификатов возникают следующие проблемы:

a) получатели заранее неизвестны отправителю;

b) получатель не знает, как верифицировать подлинность полученных данных.

Обе проблемы решаются одинаково. Аутентичный перечень уполномоченных контактных лиц в каждом государстве, который называется "Реестр CSCA".

A8.2 Реестр CSCA представляет собой список подробных контактных сведений о CSCA каждого государства, выдающего или считывающего электронные МСОПД, включая конкретную информацию о CSCA, в которой МОГУТ быть:

a) полное имя, почтовый адрес и электронный адрес лица, отвечающего за функционирование CSCA;

b) сертифицированный CSCA отпечаток большого пальца;

c) способ получения сертификата CSCA;

d) сервер LDAP содержащий сертификаты и CRL, выпущенные CSCA;

e) номер факса;

f) веб-сайт, содержащий (дополнительную) информацию о CSCA, например о политике в отношении сертификатов и/или заявления о практике в отношении сертификатов.

Полномочным органам выдачи РЕКОМЕНДУЕТСЯ пополнять информацией реестры CSCA. Полномочным проверяющим органам РЕКОМЕНДУЕТСЯ консультироваться с реестрами CSCA для получения информации о CSCA и CRL.

– КОНЕЦ –

ISBN 978-92-9231-310-4